Number 8 (Third edition)
June 2025

Humanitarian Practice Network

Good Practice Review

Humanitarian security risk management

Published in collaboration with Humanitarian Outcomes

Humanitarian security risk management

Good Practice Review 8
Third edition

Humanitarian
Practice
Network

Humanitarian Practice Network (HPN)
ODI Global
4 Millbank
London SW1P 3LL
United Kingdom

Email: hpn@odi.org.uk
Website: www.odihpn.org

Printed and bound in the UK by Formara Print and Marketing
Layout and production: Jessica Rennoldson

ISBN: 978-1-0682923-0-9

Good Practice Review

Humanitarian security risk management

June 2025

Third edition

Contents

Authorship and acknowledgements

This revised *Good Practice Review* (GPR) is dedicated to the many humanitarian security specialists who work tirelessly to support their colleagues and organisations. It is dedicated to those no longer with us, whose contributions and dedication to this field will always be remembered.

This third edition was co-edited by Adelicia Fairbanks and Abby Stoddard from Humanitarian Outcomes. They were supported by Monica Czwarno and Meriah-Jo Breckenridge, also from Humanitarian Outcomes. Samiha Ahmed coordinated the production process for HPN, and Matthew Foley, Editor at ODI Global, edited the manuscript. This GPR builds on the work of previous editions, led by Koenraad Van Brabant, Adele Harmer, Abby Stoddard and Katherine Haver.

Contributors to this GPR generously gave their time to review content, provide resources, share knowledge and advice, and contribute to the writing. This GPR is truly a collective effort, with contributions made by:

Banu Altunbas

Tara Arthur, Collective Security Group

Javeria Ayaz Malik, ActionAid and INSSA

Petro Babyak, Mercy Corps Ukraine

Shaun Bickley, Tricky Locations

Awil Bihi, CARE

Tamsin Blake, Medair

Donald S. Bosch, Ph.D., Psya.D., Humanitarian Psychological Services

Phil Candy, Medair

Araba Cole

Amaury T. Cooper

Gonzalo de Palacios, Oxfam

Steve Dennis, Proper Support Recovery Consulting

Catherine Deseure-Plumridge, UNDSS

Gurpreet Dhoot, Fauna & Flora

Neil Elliot, MSyl, Oxfam International

Daniel Elliott, CAFOD

Shannon Fariel-Mureithi, ChildFund International

Anthony Val Flynn, European Commission Directorate General for International Partnerships

Alexandra Godoi, Oxfam GB and Oxfam International

Paul Herridge, Itad

Henrieke Hommes, ZOA

Heather Hughes, Global Interagency Security Forum (GISF)

Stephen Ingram, Mines Advisory Group

Rafael K. Khusnutdinov, RTI International

Jean-Philippe Kiehl, International Committee of the Red Cross

Sarah Kilani, Centre on Armed Groups

Jenna Kuokkanen, World Vision International

Elodie Leroy-Le Moigne, Plan International

Armstrong Maina, Project HOPE

Steven A. Mercer, Samaritan's Purse International Relief

Alan Mordaunt, Trócaire

Robert Muggah, Igarapé Institute

Noemi Muñoz Zamora, International Rescue Committee (IRC)

Michael O'Neill, INSSA

Kevin Pedone, Clements Worldwide

Carina Peña, World Food Programme

Christine Persaud, University of Québec, Montreal

William Plowright, Durham University

Adrian Powell, Proelium Law LLP

Pegah Rajabi, International NGO Safety Organisation (INSO)

Jeremy Reeves

Lisa Reilly

Jochen Riegg, Norwegian Refugee Council

Scott Ruddick, Cowater International

Rod Slip, Oxfam

Craig Spencer, M.D., M.P.H., Brown University School of Public Health

Barry Steyn, International Rescue Committee (IRC)

Matt Stockton, Global Interagency Security Forum (GISF)

Sandrine Tiller, Médecins Sans Frontières

Marieke van Weerden

Julian Visser, ZOA

Ron Waldman, MD, MPH, Milken Institute School of Public Health, George Washington University

Benjamin Whelan, Access Now

Christina Wille, Insecurity Insight

Chris Williams, CARE

Christine Williamson, Duty of Care International

Ian Woodmansey, Crucial Safety

Tara Yip-Bannicq Ward, Plan International

Hannah Zitner, International Rescue Committee (IRC)

Disclaimer to this Good Practice Review ('GPR')

ODI Global will to the fullest extent permitted by law:

1. Not make or imply any representation, promise or warranty as to the guidance or advice provided in this GPR.
2. Not make, imply or warranty as to the quality, life or wear of this GPR published in 2025 nor that it will be suitable for any particular purpose or for use under any specific conditions.
3. Assume no liability or responsibility for any loss, damage, or inconvenience arising as a consequence of any use of or the inability to use, or interpretation of, any information contained within this GPR.
4. Not assume any duty of care, responsibility and will not be liable to you, or anyone else, for any damages whatsoever incurred for any decisions made or action taken in light of information provided in this GPR.

Any information in this GPR is presented by ODI Global or its third-party collaborators who have contributed to this GPR as their understanding at the time of publication of security risk management guidance for general purposes. This GPR must not be regarded as an adequate or valid statement about any standard operating procedures, threat patterns in a particular country or the security risk management of one or more agencies.

Although ODI Global has endeavoured to ensure the accuracy and quality of the information presented in this GPR, ODI Global cannot guarantee the accuracy or quality of the information presented in this GPR. You must do your own assessment as to the risk and behaviour to adopt in high-risk, violent or potentially high-risk or violent environments, even in the conditions described in this GPR. This GPR cannot under any circumstances replace your obligations to make your own due diligence or assessment before operating in any violent, high-risk or potentially violent or high-risk environment. This GPR is made public on a non-reliance basis.

This GPR may include the views or recommendations of third parties and does not necessarily reflect the views of ODI Global or indicate a commitment to a particular course of action.

Glossary of security terms

The following glossary contains key terms and concepts relevant to this *Good Practice Review*.[1]

Abduction Any illegal, forcible capture of a person or group.

Acceptance analysis A process of evaluating the levels of acceptance the organisation has among different stakeholders in the environment.

Acceptance approach An approach to security risk management that attempts to reduce or remove threats through building relationships with local communities and relevant stakeholders in the operating area and obtaining their goodwill and/or consent for the organisation's presence and work.

Actor analysis/mapping An exercise to identify and analyse the actors/stakeholders in a given environment that are key to contextual understanding and that may affect an organisation's security.

Anti-surveillance The practice of detecting surveillance, for example to determine if staff movements or facilities are being studied with malicious intent.

Arrest The seizure and detention of an individual by a formal authority (police or military) in connection with a crime, offence or infraction.

CBRN Chemical, biological, radiological and nuclear threats/weapons.

Civil–military coordination Interaction between military forces and humanitarian organisations/civilian actors necessary to promote humanitarian principles, secure access and protect aid workers and other civilians.

Communications tree A hierarchical system used to quickly disseminate information to a large group by phone, text, email or other means.

Context analysis A process of understanding the environment in which an organisation operates as a first step to identify potential security threats and vulnerabilities.

1 This glossary adapts and aligns with the Global Interagency Security Forum (GISF) Glossary: https://gisf.ngo/glossary-english/

Contingency plan A set of pre-established procedures and measures adapted to the local context that guide staff in coordinating a rapid and effective response to specific security incidents or disruptions.

Convoy A group of vehicles (or ships) travelling together in an organised manner for mutual support and protection.

Crisis An event or series of events that significantly disrupts an organisation's normal operations and has severe consequences for individual staff or the organisation, requiring extraordinary measures and immediate action from senior management.

Critical incident An event or series of events that seriously threatens the welfare of personnel, potentially resulting in death, life-threatening injury or illness. A critical incident may be too severe to be handled through standard management structures, and requires additional support and capacities.

Deconfliction The exchange of information between humanitarian actors and military forces to prevent attacks on relief facilities, personnel and operations by notifying parties to a conflict about the locations and movements of humanitarian staff and activities.

Detention The holding of a person against their will by a person or group but without formal charges, a clear timeline or conditions for their release.

Deterrence approach A security approach that involves reducing or removing threats by posing a counter-threat that will deter or influence would-be aggressors.

Digital security Measures, strategies and processes that aim to mitigate risks related to the use of digital technologies and an individual's and/or organisation's digital presence and behaviours.

Duty of care An organisation's obligation (moral and legal) to the safety, security and wellbeing of the individuals carrying out its work.

Enterprise risk management An organisational process of identifying and managing all risks, including but not exclusive to security risk, that could impact its objectives, operations and stakeholders.

Evacuation Withdrawing staff for security reasons to a place of safety across the international borders of a country.

Extortion The use of coercion, threats or intimidation to obtain money, property or actions from the target.

First aid Provision of immediate assistance to an ill, injured or emotionally distressed person ('psychological first aid') until professional help is obtained.

Harassment Continued abusive or unwanted conduct directed at a person, which causes distress or discomfort.

Hate speech Written or spoken content that targets a group or individual based on their inherent characteristics, such as ethnicity, religion or gender.

Hibernation Temporarily ceasing regular project activities while having staff remain at the office, home or other safe location to avoid an emerging threat, or until conditions improve.

Hostage situation The holding of a person or group by force in a known location, such as in a siege situation, until specific demands are met.

Hostile environment awareness training (HEAT) Personal security training designed for staff working in high-risk environments, usually involving scenario-based training.

Hostile surveillance The close observation of individuals, assets or properties with malicious intent, such as planning for an attack.

Humanitarian access The ability of humanitarian actors to reach affected populations, and affected people's ability to access assistance and services.

Identity-based risks The risks to staff as a result of their personal characteristics and how these are perceived.

Incident An adverse security event that results in, or could result in, harm to staff, disruption to programmes and activities, or loss of or damage to the organisation's assets or reputation.

Information security The practice of protecting information from unauthorised access, theft, disclosure, disruption, modification or destruction.

Intersectional identity The multiple interconnected identity factors of individuals that shape their personal risk profiles.

Kidnapping The forcible capture of a person or group who are held against their will in an unknown location until demands for a ransom payment or other concessions are met.

Medevac Medical evacuation. The movement of a patient by road, sea or air by specialist medical transport, with care provided en route, for the purpose of obtaining medical treatment in another location.

Minimum security requirements Protocols that the organisation expects all staff to follow to ensure the safety and security of assets, personnel and information.

Mis-, dis- and malinformation Misinformation is inaccurate or false information that is shared without the intent to deceive. Disinformation is information that is deliberately false or misleading. Malinformation is true information that is taken out of its original context or manipulated in a way to mislead or cause damage.

Partnership Any formalised working relationship between two or more organisations to meet agreed objectives, as in the implementation of an aid programme.

Person-centred approach to security A security risk management approach that places individuals at the core of security risk management activities and considers their personal risk profiles. It recognises the profile-specific risks that individuals face due to their intersectional identity, their behaviour, their role and organisation and the context in which they are working.

Personal risk profile The unique set of risks an individual faces based on their intersectional identity, which is shaped in part by how their personal characteristics are perceived by others.

Private security provider/company A private entity providing remunerated security services to individuals or organisations.

Programme criticality A measure of how much people's lives or freedom from extreme suffering rely on the aid activity continuing.

Protection approach A security approach that seeks to reduce staff exposure to certain threats through protective mechanisms and procedures.

Psychosocial support An approach that integrates both psychological and social aspects of wellbeing, addressing the impact of relationships, environment and community on mental health.

Ransom Money, goods or services demanded or paid in exchange for the safe release of abducted individuals.

Relocation Withdrawing staff and assets from insecure locations to safer areas within the country, until the situation stabilises.

Residual risk The level of risk remaining after all appropriate risk mitigation measures are taken.

Risk The likelihood of something harmful happening, and the extent of that harm if it does.

Risk appetite A shared understanding of the amount and type of risk that an organisation is prepared to accept to meet its goals.

Risk assessment/analysis A multi-step analytical process through which organisations identify risks to their staff, assets, programmes and reputation, and evaluate them according to their likelihood and impact to determine their severity.

Risk levels/ratings Evaluated risks, classified by their degree of severity in terms of likelihood and impact.

Risk mitigation Actions to reduce risks by reducing the likelihood and the potential impact of harm.

Risk sharing Sharing responsibility equitably between organisational partners for the risks that affect them both.

Risk threshold The limit of acceptable risk, beyond which the organisation, or an individual, is unwilling to go.

Risk transfer The intentional or unintentional creation, transformation or shifting of risks from one actor to another.

Safety Freedom from risk or harm as a result of unintentional acts (accidents, natural phenomena or illness).

Saving Lives Together (SLT) A framework for security collaboration between the UN Security Management System (UNSMS), international non-governmental organisations and other international organisations globally, and in shared humanitarian response settings.

Security Freedom from risk or harm resulting from violence or other intentional acts.

Security audit An internal or external evidence-based review that assesses the effectiveness of the organisation's security risk management and whether it is meeting its duty of care responsibilities to staff.

Security collaboration Organisations acting together to address common concerns regarding security and access, share information on incidents and risks and strengthen their collective risk management capacities.

Security culture Shared assumptions, values and beliefs that shape behaviour around security in organisations. Can be positive or negative.

Security incident information management The process of collecting and using information related to safety and security incidents to monitor trends and inform decision-making.

Security levels A system used to categorise and communicate the level of risk to staff in a specific context or location and to guide security risk management decisions, actions and measures in response to increasing insecurity (also referred to as security phases).

Security plan A location-specific document, or set of documents, outlining the measures and procedures in place to manage security, and the responsibilities and resources required to implement them.

Security policy A governance document that states the organisation's approach to security and safety risks, the key principles underpinning this approach, and the roles and responsibilities all staff members have in managing risks.

Security risk management An organisational system for assessing and mitigating risks and responding to incidents.

Security risk management framework A set of policies, protocols, plans, mechanisms and responsibilities that supports the reduction of security risks to staff.

Security staff/focal point A staff member with responsibility for safety and security within their scope of work.

Security strategy An organisation's approach to managing security depending on the operating environment and the risks in that location, influenced by the organisation's principles and values.

Sexual violence Any sexual act that is forced, coerced or happens without consent.

Standard Operating Procedures (SOPs) A set of step-by-step instructions to assist staff in undertaking routine operations or responding to specific situations in a way that maximises safety and security.

Stress An emotional, cognitive, physical or behavioural reaction to pressures and challenging situations.

Survivor-centred approach A focus on prioritising the needs, rights and safety of individuals affected by traumatic events. It emphasises respect, confidentiality and autonomy, allowing survivors to make informed decisions while recognising their potential need for support through the recovery process.

Threat Any event, action or entity with the potential to cause harm to personnel, programmes or assets, or hinder the achievement of aid objectives.

Threat assessment A process of identifying and analysing potential sources of harm in an operating environment.

Trauma A distressing or disturbing experience that overwhelms an individual's ability to cope and has lasting adverse effects on their functioning and wellbeing.

Vulnerability assessment A process of analysing the degree to which an organisation's staff, properties and assets are exposed to threats.

Foreword

The first edition of this *Good Practice Review* represented the collective knowledge of humanitarian and non-governmental organisation (NGO) aid workers who had gathered in 1998 – first in the United States (US) and later that year in the United Kingdom (UK) – for a week-long security training, reflecting the growing recognition that we, as a community, needed to collaborate if we were to improve our approach to institutional security management. A fully collective endeavour, the preparation and development of 'GPR8' engaged humanitarian and development workers, peacebuilders, engineers, trainers, deminers, theoreticians and a handful of NGO security management professionals striving to address the security management challenges of the day. GPR8 became the seminal textbook providing templates and guidance for a generation of NGO and humanitarian security managers and security focal points.

The revised edition of GPR8 in 2010 acknowledged the valuable input from a host of humanitarian and NGO security management professionals, many of whose positions had not existed when the first edition was published in 2000. Their experiences applying the principles and guidance presented in the original text reinforced good practice and led to improved approaches and refined tools. Among the topics highlighted were improved risk assessments, implementing an 'active acceptance' approach, exploring security dimensions of 'remote management' programming, promoting interagency security coordination, and managing critical incidents.

Building on the previous editions, this third GPR8 draws on the knowledge and experience of the last 15 years, incorporating findings from recent research on existing and emergent approaches to the management of security risks. It also reflects the many significant changes to the broader humanitarian landscape over this period. One of the most important is the overdue recognition of the important role of national actors in humanitarian response and humanitarian security risk management ecosystems, as well as the specific challenges they face.

This version clearly highlights that good security risk management is needed in all humanitarian response contexts – not just the most violent environments – and encourages readers to engage in critical thinking about where and how threats and risks emerge, and who is deemed threatening and why. Key to this is

acknowledging that the boundaries between programming locations and other, supposedly safe, spaces such as home, head office, sub-office and compound are porous. An important new element of this edition concerns the concept and application of a person-centred approach to security risk management. This approach encourages security risk management professionals to focus as much on 'who is safe' as on 'where is safe', leading to a better understanding of the importance of identity-based risks.

The new edition also addresses: security risk management within implementing partnerships and remotely managed operations; the relevance of new technologies to security risk management; training needs, types and sourcing; and how security risk management can be affected by – as well as feed into – external advocacy work.

We hope this updated and expanded GPR8 will support humanitarian responders to identify and manage security risks more effectively. The dynamic nature of the operational environment, compounded by global phenomena that will likely displace millions of people in years to come, demands that we constantly reflect and assess anew the core principles of effective security risk management and the means of putting these into practice.

Wendy Fenton
Former HPN Coordinator

Michael O'Neill
International NGO Safety and Security Association (*INSSA*)

Introduction

Published in 2000, the *Good Practice Review on Operational Security Management in Violent Environments*, or 'GPR8', quickly became a staple in the nascent field of security risk management of humanitarian operations. At the time, very few organisations had dedicated staff or developed mechanisms for security, and the publication served as both a wake-up call on the need to better manage risks, and a template for many organisations' early efforts.

A revised edition in 2010 saw the inclusion of updated examples, reflecting changes in the humanitarian sector and in the threats humanitarians were facing in the post-9/11 landscape of conflict and crisis.

Although the concepts and principles introduced in these first two editions remain valid, another decade and a half has elapsed, humanitarian capacities and security environments continue to evolve, and new thinking in security risk management merit another revision. While no longer the sole, indispensable resource it was at the time of its first publication, GPR8 can serve as a foundational text and a useful compendium of principles and practice for humanitarian security risk management experts and newcomers alike.

Background to the new edition

As with the two previous editions, this version of GPR8 is the result of the combined efforts of a large number of practitioner-experts. As a collaboration between Humanitarian Outcomes, the Global Interagency Security Forum (GISF) and the Humanitarian Practice Network (HPN), the project to update the volume began in 2022, with funding provided by the US Agency for International Development's Bureau for Humanitarian Assistance (USAID/BHA).

As a first step, the editorial team conducted a global survey of humanitarian security risk management professionals to gauge GPR8's current usership and relevance. The survey revealed that most security staff were familiar with the publication, with more than a quarter continuing to include it in staff informational materials. There was also support for a third edition. However, the survey confirmed that, with the proliferation of technical guidance and 'how-to' materials on security risk management, GPR8 is now valued more as

an authoritative reference for security staff and a primer on key concepts and principles for those new to the subject, rather than as a practical handbook.

With this in mind, the team embarked on an in-depth study of current practice and new thinking in security risk management in humanitarian contexts. The research encompassed case-based research in five humanitarian contexts (Central African Republic, Colombia, Ethiopia, Iraq and Ukraine) and consultations with more than 250 humanitarian practitioners globally. The findings, published as a separate report by GISF and Humanitarian Outcomes in 2024, informed much of the new content in this volume, along with the separate contributions and critical reviews provided by participating experts.[1] From the start, the project has been guided by an advisory group of major stakeholders and thought leaders in security risk management. Each chapter was reviewed and revised by the editors, then shared with a group of subject matter experts for their substantive input. In addition, some new chapters were written by participating experts and underwent the same peer review process. After incorporating the feedback, revised drafts were reviewed for overall content, structure, technical accuracy and sensitivity of language and tone.

What's new

In addition to a shortened title, covering non-operational aspects of security risk management and reflecting the reality that security risks can exist in all sorts of environments, this edition updates the content of earlier versions and introduces new topics, informed by the latest research and thinking in the sector. Notably, it introduces and applies the concept of a 'person-centred approach' to security risk management, which places the individual at the centre of security risk management. The new edition also emphasises the critical work and disproportionate risk burden of national and local humanitarian actors, and discusses how security risk management functions within national–international partnerships.

New topics include the security dimensions of access and deconfliction efforts, as well as the new array of digital risks facing humanitarian organisations in the form of mis- and disinformation, data theft, surveillance and cybercrime. There is also new content relating to general criminality, and additional content on training, funding, compliance and duty of care. The revised structure of the

1 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).

volume recognises that security risk management takes place within different ecosystems – the organisation, the humanitarian system and the wider aid space and political arena – each with its own considerations and challenges.

This edition of GPR8 emphasises good practice and guiding principles over providing step-by-step instructions on technical procedures. The abundance of new, mostly online resources in the humanitarian space providing detailed guidance amply meet this need, and trying to replicate them would make the volume superfluous and quickly out of date. Instead, it focuses on introducing ideas and concepts to encourage reflection and inform higher-level policy discussion, and sharing good practice from experts, while pointing the reader to relevant resources for concrete examples, templates and practical guidance.

Finally, the editors and contributors to this revision sought to de-centre as much as possible the western international organisation as the principal perspective of – and audience for – this material, in an effort to ensure that the language and the approach to the content was relevant to – and inclusive of – all humanitarian aid providers.

Target audience

The original GPR8 was aimed primarily at senior operational managers in humanitarian organisations overseeing operations in hostile environments. This edition targets a somewhat broader audience. First, it takes care to include all humanitarian organisations – local, national and international, ranging from very small to very large. Because organisations of different sizes and budgets have different needs and capacities, however, some of the good practices described for large organisations with multiple departments and offices may be less relevant or feasible for smaller organisations to implement. Where possible, this is noted in the text with a reminder of the core principles behind these practices, which are universally applicable.

In addition to humanitarian staff with security responsibilities (referred to as 'security staff' throughout), the GPR may be relevant for senior leadership and boards of humanitarian organisations, as well as students, journalists, researchers and anyone interested in learning more about security risk management for humanitarian operations. Other organisations operating in conditions of risk may also find it useful.

The good practices described here pertain to security risk management at the organisational level, intended for consideration by staff responsible for enhancing the security of all staff members. The GPR is not written for individual staff regarding their personal safety or actions to take during an incident. This does not diminish the importance of individual agency in security, but simply reflects the scope of the guidance.

The term 'staff' refers to any individuals working on behalf of the organisation, including volunteers. The umbrella term 'organisations' includes aid organisations of all kinds, from United Nations (UN) agencies and the Red Cross/Red Crescent Movement to NGOs and community-based organisations. The diversity of humanitarian actors means that, occasionally, some of the content may be more or less relevant to a particular type of organisation. Again, by emphasising foundational principles and reflection, we hope this guide can be of some value to all.

To keep in mind

The central subject of this volume is 'security', which concerns deliberate acts to cause harm (such as violence and crime), as opposed to 'safety', which implies accidents or other circumstances that result in unintentional harm (such as fires and environmental hazards). Though in practice the two often overlap, this volume does not go into depth on safety-related aspects of humanitarian action.

The GPR deliberately uses non-prescriptive language, offering good practices for staff with security responsibilities to consider, rather than setting forth any standards or requirements. All practices described are intended to be adapted to fit the specific needs and operational contexts of each organisation.

In humanitarian crises, the general public is often at equal or greater risk of violence compared to aid workers, and in need of major assistance and protection. However, the strategies used to protect affected people are often quite different from those used to protect aid workers, and also fall within the responsibilities of separate departments to those of security risk management within most organisations.

Finally, it is important to recognise and reinforce the understanding that achieving effective security risk management is not an end in itself. Rather, it is a means to achieve the broader goal of addressing the humanitarian needs of people in crisis.

How this review is structured

We begin with broad, foundational principles of humanitarian security risk management, then delve into more specific areas of practice. Newcomers to security risk management can follow the chapter order for a comprehensive introduction to the subject, but each section is self-contained and can be read independently.

Part 1 explains key concepts such as threat, risk, duty of care and programme criticality, introducing the latest thinking on the person-centred approach to security. **Part 2** describes the 'ecosystems' in which security risk management takes place – the operational context, the interagency community and joint mechanisms, the wider circle of actors such as governments and militaries, and the interaction with other organisational objectives such as advocacy. **Parts 3 and 4** then discuss the major strategic, policy and operational elements of developing and implementing an organisational security risk management system. **Part 5** covers issues related to human resources, good practices in communication, training and staff wellbeing. **Part 6** is devoted to security risk management in the area of information and communications technology, including harmful information. Finally, **Part 7** provides examples of risk mitigation for specific situations and types of threat. These have been revised and updated to reflect recent trends in insecurity and current operational contexts.

1 Foundations of humanitarian security risk management

1.1 Key concepts and principles

This chapter introduces the foundational ideas of security risk management for humanitarian action. These include the basic concepts of threat and risk, duty of care and risk thresholds, as well as how they correspond to programme criticality. The chapter also describes the foundational principles of humanitarian action and how they relate to security, and good practice in creating an organisational security culture.

1.1.1 What are security risks, and what does it mean to 'manage' them?

Humanitarian action, which often takes place amid instability, conflict and crisis conditions, inevitably entails some security risk. While risks can never be completely eliminated, their effective management can make the difference between people receiving lifesaving aid or not.

Insecurity is only one type of risk that people and organisations may face. There are many others, including financial, operational, fiduciary and reputational risk – all of which can interlink with each other and with security risk. The definition of risk more broadly, according to *ISO 31000*, is 'the effect of uncertainty on objectives'.[2] Implicit in this definition are two important distinctions – that a risk is not the same thing as a threat, and that, while managing risk is linked to objectives, it is not synonymous with them. In the humanitarian context, therefore, security risk management is ultimately in service to humanitarian objectives; avoiding harm and loss is a means, not the end in itself. This is important because, when 'keeping people safe' becomes the over-riding goal, risk aversion is the inevitable result.

Key concepts to understand are:

- Threat
- Vulnerability
- Risk
- Risk mitigation/reduction.

2 International Organization for Standardization (2018) *ISO 31000:2018: Risk management – Guidelines*. (www.iso.org/standard/65694.html).

In an operational environment, a threat is anything that can cause harm or loss, while vulnerability refers to the likelihood of being confronted with a threat, and the impact that would result. The combination of a security threat and one's vulnerability to that threat constitutes security risk. In other words, security risk is about the potential for harm: the likelihood of something harmful happening, and the extent of that harm if it does.

An organisation can choose to avoid certain risks entirely (for example, deciding not to work in a given area), and it can transfer the risk to someone else, such as a contractor or implementing partner – more on this later. But when doing direct programming and seeking to reduce and mitigate the risks to its staff, there are three main types of measures an organisation may take, none of which is mutually exclusive:

- Neutralising the threat – diminishing the threat itself (such as negotiating safe access agreements with an armed group to reduce hostility).
- Reducing likelihood – reducing exposure to the threat.
- Reducing impact – taking measures to ensure that, when confronted with the threat, the impact will be limited.

Beginning around 2000, the humanitarian sector has developed and operationalised a body of knowledge, policies and practices known as 'security risk management' – the subject of this volume. Security risk management is an organisational system for identifying, assessing and preparing for risks to help prevent security incidents from happening and to minimise their impact when they do by responding to them effectively. By taking active measures to reduce security risks, an aid organisation is maximising its ability to meet its programmatic objectives while also upholding its duty of care to the people providing the aid.

At its core, security risk management in the humanitarian space is an enabler of safe access. There can be no access without some degree of protection for staff members that enables them to work within reasonable and agreed risk thresholds. When security risk management is effective, it ensures that staff assist people in need and that they feel safe and confident in executing their work. This, in turn, can help fulfil organisational responsibilities towards personnel, bolster the organisation's reputation as a legitimate partner to donors as well as limiting losses, and expand an organisation's scope and competitive edge. Simply put, security risk management becomes a powerful core enabler of the organisation's overall strategic and programmatic objectives.

1.1.2 Duty of care

Duty of care refers to an organisation's obligation to the safety, security and wellbeing of the individuals carrying out its work. The concept has important legal and moral implications for aid organisations. In the strict legal sense, duty of care is the requirement for organisations to take all reasonable and appropriate measures to enhance the safety and security of their staff. Many countries have incorporated duty of care into labour laws and other legislation. Failure to fully inform staff about risks and to take reasonable risk mitigation measures can expose an organisation to claims of negligence and legal liability. More importantly, neglect of this duty can result in devastating or fatal consequences for individuals.

While there is no single, standard set of actions that define a duty of care policy, there are common elements of good practice:

- Undertaking assessments of the risks to staff of any new conditions, locations or activities in which they will be working.
- Informing staff of the risks they may face, what the organisation has put in place to address those risks, and what actions individuals themselves are expected to take (including behavioural expectations).
- Working to prevent incidents from occurring, such as by putting in place risk mitigation measures based on assessed risks.
- Monitoring the implementation and relevance of security risk management measures.
- Intervening in the event of an incident to reduce the negative outcomes, for example by setting up crisis management teams and providing post-incident care to affected staff.

As later chapters will detail, the above are closely linked with activities integral to good security risk management. It is important to note that duty of care can also fall outside of the formally established employer–employee relationship. Organisations engage consultants, volunteers and a range of service providers where duty of care may not be automatically owed, but to whom they may still have some responsibility. An organisation's legal responsibility may be understood, depending on the jurisdiction, as relative to the degree of control it has over a person in a given environment, such as their accommodation, location and choice of transport.[3]

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

Increasingly, organisations are developing duty of care policies and frameworks to strategically guide these different aspects of staff care, and to communicate to staff the organisation's commitment to their overall wellbeing. This includes adapting duty of care policies to cater to a diverse workforce, considering different personal and cultural backgrounds, which may affect security risk. These policies can be regularly revisited to reflect new challenges and circumstances.

Duty of care framework example

A number of processes support duty of care, and a framework can help to visually communicate what these are. One organisation has structured its duty of care framework with 'culture' (shared values and wellness goals) at the centre, and operational security as one of many supporting inputs, including governance, training, communications and crisis management. Figure 1 is an example duty of care framework developed to help delineate and convey the intent of duty of care, with safety and security as a distinct element within it.

Figure 1 Visualising the duty of care framework

Culture – values, ways of working, engagement and inclusivity, wellbeing.

Governance, leadership and accountability – setting policy, providing clarity around risk appetite and threshold, and establishing structures for oversight, accountability, transparency and learning.

Operational safety and security – location-specific and activity-specific risk assessments and security plans, travel risk management, inclusive of personal identity risks and source/partner/interlocutor commitments.

Crisis management – people, plans, insurance and consultants, training, communication, pre- and post-incident support and after-action reviews.

Resources – funding, staffing and consultancy support.

Communication – methods, protocols, information security, devices, licences, training and drills.

Training – onboarding, personal and team safety and security and security risk management.

Central to duty of care are good communication and informing staff about risks. Organisations have a responsibility to inform personnel and potential personnel (including volunteers and consultants) about the security risks they may face and what mitigation measures will be used. Full engagement on these matters allows individuals to make an explicit, deliberate and informed decision on whether to accept the risks identified.

Ensuring communication and staff engagement can involve the following:

- **Comprehensive disclosure of information**. This includes details about the specific nature of the risks, the security measures in place, individual roles and responsibilities, and any potential health and safety implications. It could also usefully indicate where information is weak or lacking.

- **Explicit discussion and acceptance of the risk.** A free and fully informed decision by staff to accept work-related risks stems from a clear understanding of the risks and mitigation measures, absent any pressure or fear of negative consequences for declining. Making this decision explicit helps ensure that both the organisation and staff are engaged and mindful of the seriousness of the situation.
- **Documentation.** It may be advisable for staff members' understanding and acceptance of the risk to be explicit and documented, particularly when security situations change, or when staff begin working in new locations. It is important to understand that this process is intended to ensure that the discussion happens, and staff are fully informed and engaged. It is not a protection against potential legal liability. While some organisations ask staff to sign 'informed consent' documents or other waivers of liability, these are not equally recognised across different legal jurisdictions and do not necessarily prevent individuals who have signed them from bringing claims of negligence.
- **Ongoing communication.** Organisations should aim to provide updates about any changes in the risk assessment, informing staff of new risks as they arise.
- **Right to withdraw**. Staff should be regularly reminded that they have the right to change their mind and discontinue their participation at any point if they feel unsafe or if conditions change significantly.

Security risk management is often an exercise in balancing the organisation's humanitarian objectives with its duty of care. At the same time, good security risk management is vital to fulfilling duty of care, and good duty of care can likewise bolster security risk management by creating conditions where staff are well informed of risks and feel valued and supported. For this to happen, the organisation must view and convey its duty of care as a core value, not as a means to avoid lawsuits and reputational damage. Lawsuits, nevertheless, are a reality. The landmark case of Dennis v. Norwegian Refugee Council (NRC) confirmed the legal liability aid organisations have towards their staff in terms of security (see example below).

Case example: Legal duty of care – lessons from the Dennis v. NRC ruling

In 2012, several aid workers were attacked during a visit to a refugee camp in Dadaab, Kenya, while working for NRC. One staff member died, and four others were kidnapped. The abductees were rescued four days later. In 2015, Steve Dennis, who had been among those kidnapped and injured during the attack, sued NRC for compensation. The Oslo District Court ruled that NRC acted with gross negligence and awarded damages to Dennis.

This case has been described as a landmark ruling and many have viewed it as a watershed moment, leading many aid organisations to strengthen their security risk management systems. While legal duty of care can vary across jurisdictions, this case's lessons can still guide organisations seeking to improve their security risk management and duty of care processes.

Some key lessons from the Oslo court's ruling were as follows.

- **Scope of duty of care:** Duty of care is as much a legal obligation for aid organisations as for any other employer, requiring mitigation measures to be proportionate to the risk.
- **Foreseeability of the risk and reasonable mitigation measures:** NRC failed to properly assess foreseeable kidnap risks, mitigate identified risks, follow security guidance (internal and external) or consult security specialists to inform key decisions.
- **Informed consent:** Staff were not informed of risks, asked to consent or able to withdraw when security plans changed.
- **Community practice:** Given the absence of concrete, universally applicable security standards in the aid sector, the court looked to aid community practices in Dadaab to understand if and how the decisions and practices of NRC differed from its peers. While deviating from commonly accepted practices is not inherently a failure, any such deviation should be a carefully justified decision based on sound reasoning and factual information.

In summary, the Oslo District Court's ruling emphasised the need for robust risk assessments and corresponding reasonable security measures by humanitarian organisations as part of their legal duty of care.

Sources: Hoppe, K. and Williamson, C. (2016) 'Dennis vs Norwegian Refugee Council: implications for duty of care'. Humanitarian Practice Network (https://odihpn.org/publication/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/); and Merkelbach, M. and Kemp, E. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF) (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

Strongly upholding duty of care is connected to overall organisational success. More broadly, duty of care can contribute to employee satisfaction and retention and organisational reputation, which in turn can support the organisation's broader goals. It is important to emphasise that most serious incidents in the aid sector do not result in court cases; the Dennis v. NRC case is well known because it is exceptional. There is evidence that a major impetus for pushing for legal redress in the Dennis v. NRC case included staff care failures following the incident, including a lack of information and transparency over what happened and follow-up measures. While not all risk can be eliminated, organisations do have control over how staff are supported following an incident, and this post-incident support is an important aspect of duty of care.

▶ *For more on post-incident care, see Chapter 5.4 – Staff care.*

Recent years have seen the term 'duty of care' applied to the ethical obligations that international organisations have to their local partners and sub-grantees. While an organisation may not be held legally responsible for people employed by other entities, it is clear these partnerships often involve a significant transfer of risk, making it incumbent on organisations to provide all possible appropriate support to their partners for the care of their personnel.

▶ *To learn more about risk transfer and partnerships, see Chapter 3.5.*

1.1.3 Residual risk, risk thresholds and programme criticality

Participating in humanitarian response efforts requires a readiness to take some risks. An organisation's risk appetite will be shaped by its strategic objectives, mission and culture, and amounts to a shared understanding of the level of risk that is appropriate to achieve the organisation's goals. Risk threshold is a shared understanding of the limit beyond which the organisation is unwilling to go. When determining this threshold, it is necessary to understand residual risk. This is the level of risk that remains after all appropriate risk mitigation measures are taken – a concept that entails acknowledging that some risk will always remain. Setting the threshold of acceptable risk as an explicit and transparent decision can help govern all other management decisions regarding what to do when faced with risk. There are three important moments when the threshold of acceptable risk should be discussed:

- When deciding to enter or expand into a risky environment.
- To determine individual thresholds of acceptable risk.
- To draw red lines (clear boundaries or thresholds) for when a situation deteriorates.

In the first case, deciding what constitutes an acceptable risk for an organisation requires explicit criteria and conditions to ensure a disciplined and transparent decision-making process.

In the second case, determining individual risk thresholds, it is important not to assume that all current and potential staff have the same threshold for what they consider acceptable risk. A climate of trust within the organisation can help people feel able to express unease if a situation exceeds their risk tolerance, and people entering a higher-risk environment must do so informed about the risks that exist there. It is also important to be aware of economic incentives or peer pressure that may lead people to take risks beyond their comfort level. Individual thresholds of acceptable risk will inevitably also be informed by personal risk profiles.

▶ *Personal risk profiles are discussed in more detail in Chapter 1.2 – Person-centred approach to security.*

The purpose of having red lines is to avoid the 'frog-in-the-pot' syndrome. When risk increases gradually, a kind of 'danger habituation' is not uncommon among

aid workers. Although there is awareness that a situation is deteriorating, staff may not withdraw from it or reinforce their security measures until after an incident has occurred. Being clear on what the trigger events or 'red lines' are can help determine when security has deteriorated significantly, and whether the programme activities clearly justify the higher risk. This introduces another key concept in security risk management – programme criticality. Programme criticality is a measure of how much people's lives or freedom from extreme suffering rely on the aid activity continuing. The more critical or lifesaving the programme, the more risk an organisation may be prepared to accept to sustain it.

1.1.4 Foundational principles of humanitarian action

By now it should be clear that security risk management is not a static formulation or set of rules to follow, but rather an elastic process where decisions will involve balancing one set of concerns against another as their relative weights change. There are other important ways in which security risk management for humanitarian operations differs from other sectors, having to do with the core humanitarian principles and the status of humanitarian workers under international humanitarian law. In armed conflicts, for example, under the Geneva Conventions and Additional Protocols, humanitarian organisations have a right to provide aid, and warring parties are obliged to facilitate their operations, protect their personnel and allow for their unobstructed movement.[4] The corollary stipulation is that humanitarian organisations operate as neutral entities, and provide aid impartially, independent of any political or other agenda, and according to need alone.

The humanitarian principles of neutrality, impartiality and independence connect directly to security by affecting how local communities and warring parties perceive aid organisations and their staff. These perceptions can make or break an organisation's acceptance (a measure by which the organisation is a known entity in a given area, and its work appreciated or at least tolerated). This in turn can impact its level of access to places where it is needed. It is chiefly through establishing acceptance that a humanitarian organisation can gain and maintain secure access to work in high-risk areas.

The 'Do No Harm'[5] principle emphasises that aid organisations must take care to avoid exacerbating existing conflicts or creating new forms of harm. This means operating in ways that minimise unintended negative consequences on the

4 For further details, see: www.icrc.org/en/document/geneva-conventions-1949-additional-protocols.

5 Anderson, M.B. (1999) *Do no harm: How aid can support peace – or war*. Lynne Rienner Publishers.

communities being served, and ensuring that programming – and, by extension, the security measures employed – does not contribute to tension, violence or inequality.

The above guiding concepts and principles are specific to humanitarian security risk management, and generally not seen among private sector, military and diplomatic actors who may share the same spaces. These foundational principles often require explanation and reiteration, both to staff and external interlocutors.

► *To learn more about the acceptance approach, go to Chapter 4.2.*

1.1.5 Developing a positive security culture

At its core, security risk management is about staff making informed decisions that safeguard their wellbeing and that of others. This can be supported by appropriate systems and tools – but it is grounded more fundamentally in shared values, beliefs and behaviours around security. An organisation whose staff have a keen awareness of security risks and actively believe that security is essential to achieving their aid objectives can be said to possess a strong or positive 'security culture'. Although culture cannot be engineered or dictated, it can be nurtured and shaped significantly by leadership and example. An organisation can set all manner of policies and procedures, but the greater part of security risk management comes in getting staff to understand and buy in to them.

Fostering a positive culture of security starts with ensuring that all staff know the organisation and its mission. Anyone working for the organisation should ideally be able to answer questions on the organisation's purpose and its activities, where it gets its funding, and its independence from any political interests.

Organisations should treat security as a staff-wide priority, not a sensitive management issue to be discussed only by a few staff members behind closed doors. Senior staff need to convey the importance they place on security risk management if they want others to follow suit. Specifically, organisations can:

- Emphasise information and communication, making security a standing item on the agenda of every management and regular staff meeting, and ensure that security is a key consideration in all programme planning.

- Stress the importance of reporting and monitoring all incidents as being vital to awareness – not as a means for blame or disciplinary action.
- Make sure that all staff are clear about their individual responsibilities with regard to security risk management and that these are included in job descriptions and performance reviews.
- Recognise and reinforce good practice, highlighting instances of good security awareness and behaviours, and where effective security risk management strategies contributed to successful operational outcomes.

▶ *See Chapter 5.1 for more detailed guidance on communication skills to improve inter-departmental collaboration.*

▶ *See Chapter 5.3 – Security communication within the organisation.*

Mainstreaming a positive security culture, both at the level of individual staff members and as an organisation, means considering the security implications involved in everything the organisation does (or chooses not to do) – from discussions about programme design and public messages to funding decisions and the hiring of external service providers. Having a positive security culture means that people consider security risks and implications in all aspects of work because they understand its importance, and are respected for doing so.

Further information

General

Anderson, M.B. (1999) *Do no harm: How aid can support peace – or war.* Lynne Rienner Publishers.

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/).

International Committee of the Red Cross (ICRC) (n.d.) *The Geneva Conventions of 1949 and their Additional Protocols* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

International Organization for Standardization (2018) *ISO 31000:2018: Risk management – Guidelines* (www.iso.org/standard/65694.html).

Duty of care

CHS Alliance (2019) *Introduction to duty of care* (www.chsalliance.org/get-support/article/introduction-duty-care/).

Duty of Care International (n.d.) *Why duty of care?* (https://dutyofcare international.co.uk/why-duty-of-care/).

GISF (n.d.) W*hat is humanitarian security risk management?* (www.gisf.ngo/about/what-is-humanitarian-security-risk-management/).

Hoppe, K. and Williamson, C. (2016) 'Dennis vs Norwegian Refugee Council: implications for duty of care'. Humanitarian Practice Network (https://odihpn.org/publication/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/).

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

Merkelbach, M. and Kemp, E. (2016) D*uty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. EISF (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

The Swiss Centre of Competence for International Cooperation (n.d.) *Duty of care under Swiss law*. cinfo (www.cinfo.ch/en/publications/duty-of-care-under-swiss-law).

1.2 Person-centred approach to security

A person-centred approach to security acknowledges that considering intersectional identity characteristics is crucial to effectively managing security risks. Rather than treating aid workers as a homogeneous group, equally vulnerable to the same threats, this approach encourages inclusivity, reflection and consideration of how the security challenges and needs of individuals are impacted by their personal profiles. This chapter discusses identity-based risks and the rationale for adopting a person-centred approach. Throughout this GPR, there are reminders and examples of how to adopt a person-centred approach to security, and this chapter should be seen as an introduction to the concept.

1.2.1 Identity-based risks

Humanitarian organisations benefit significantly from staff diversity, which enhances their ability to understand and engage effectively with diverse target communities, thereby ensuring that interventions are culturally sensitive and well received. By bringing varied perspectives, experiences and skills, diverse teams can also contribute to more comprehensive analysis and innovative problem-solving, better equipping organisations to handle crises and adapt to change. Organisations that prioritise diversity may also see higher levels of staff engagement and retention. Ensuring that organisations have adequate diversity and inclusion is therefore imperative, and a component of this is ensuring that this diverse workforce is kept safe. Fundamental to this is understanding how identity can affect risk.

It is important to emphasise that every individual has both vulnerabilities and strengths. An inclusive approach to security risk management involves challenging stereotypes that suggest certain profiles are inherently more vulnerable. These assumptions may not always be accurate and overlook the valuable contributions that a more diverse range of staff profiles and backgrounds can make to security risk management and humanitarian work as a whole. By focusing on both vulnerabilities and strengths, organisations can create a more balanced and effective approach.

Identity-based risks

The security risks staff face are affected by their identity, which is never just one thing, and, more importantly, by how their combination of personal characteristics – their 'intersectional identity' – is perceived by others.

Intersectionality describes how various social factors (gender, ethnicity, sexual orientation, socioeconomic status, disability) interact and overlap to create unique experiences of discrimination and privilege. Here, we refer to 'intersectional identity', which recognises that people have multiple interconnected identities that cannot be understood in isolation. The intersecting aspects of an individual's identity create a unique risk profile that requires a nuanced and comprehensive security approach.

While it is not possible to cover every personal risk profile, the following examples illustrate some identity-based considerations.

- **Race, ethnicity and nationality.**[6] Perceptions of race, ethnicity and nationality can influence how staff are treated within and outside an organisation. Perceptions and biases may lead to increased risks of targeted violence, discrimination, exclusion, profiling and other expressions of racism and xenophobia, depending on the context and its social dynamics.[7]
- **Disability and accessibility**. Staff with disabilities can face added challenges, such as reduced mobility or access to medical supplies and services, particularly in emergencies. They may also experience increased vulnerability to violence and exploitation, as well as social isolation.
- **Cultural and religious factors.** Language, culture and religion can impact communication, integration and security. Staff may face specific risks based on their religious beliefs or cultural differences in regions where religious or other tensions are high.
- **Gender, sexuality and identity.** Risks related to gender and sexuality affect all individuals but may be more pronounced for staff whose sexual orientation, gender identity and expression are stigmatised, restricted, marginalised, underrepresented or criminalised in the location in question. Gender can shape the nature and severity of the threats faced by staff – including within interpersonal relationships – beyond simply different risks for men and women.
- **Other considerations.** Socioeconomic status, job roles, age and previous work experience can all affect how staff are perceived and treated and, consequently, what risks they may face. Perceptions of hierarchy can also

6 We acknowledge that identity factors such as gender, nationality, ethnicity and race are socially constructed concepts. While we recognise their artificial nature, they are included here to highlight that the perception of these identity factors can lead to real and sometimes severe security consequences for individuals.

7 For a more detailed discussion, see Arthur, T. and Moutard, L. (2022) *Toward inclusive security: The impact of 'race', ethnicity, and nationality on aid workers' security.* GISF (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

play a role (within society as well as an organisation), with lower-paid staff or those in more vulnerable positions (such as drivers, cleaners or interns) potentially more exposed to danger but often with access to fewer resources and less protection. Because of perceptions and biases, individuals from underrepresented and marginalised groups may also not receive adequate attention within their organisations, which can result in insufficient security support for these staff members.

Case example: Failures in addressing identity-based risks

In a context with a predominantly white population, an international staff member with a darker complexion experienced street harassment at a higher level than some of her other female colleagues in the organisation. This not only affected her ability to move freely between home and office, but also impacted her mental health and social life outside of work.

When she voiced her concerns, the office minimised them, suggesting that such harassment was to be expected. This response made it difficult for her to report the continued and escalating harassment she faced, and the burdensome process of requesting a vehicle for safe travel further discouraged her from seeking help. Ultimately, the person chose to leave. A low-cost mitigation strategy, such as improving administrative processes to request a safe ride and fostering greater sensitivity to individual experiences, could have improved her situation and potentially retained her within the organisation.

It is crucial to underscore that how an individual is perceived is often a more important security consideration than how they self-identify. These perceptions are often rooted in biases that behavioural change cannot necessarily address. It is important to consider how intersectional identity traits of staff can contribute to, exacerbate or influence the response and behaviour of different actors, both internal and external to the organisation, towards that individual.

Additional considerations

- **Visibility.** Not all identity characteristics are visible or immediately apparent (e.g. sexual orientation and some disabilities). This demonstrates the need for an inclusive security risk management approach that by default assumes that staff have diverse security needs and accounts for this diversity to the greatest extent possible through guidance and consultative processes. It also means creating an organisational environment that empowers staff to voice concerns and seek guidance around risks relating to their identity profiles.
- **Location.** Many security risk management approaches focus on location-based risks, considering the general threats in the area. While these are undeniably important, they are not the only or necessarily the paramount consideration in all cases. With some broad exceptions (such as active combat zones or other contexts where violence is indiscriminate) whether a location is 'safe' for a staff member can often have more to do with who the person is and how they are perceived than where they are.[8] Even for the exceptions mentioned, certain profiles – such as national aid workers – are more likely to be in these locations and are therefore at heightened risk due to greater exposure. The rise of digital threats and the resurgence of major conflict in Europe in recent years are further evidence of the need to shift conversations around security away from talking about 'where is safe' to 'who is safe'.

▶ *See Chapter 6.2 for more details on how identity aspects affect digital security.*

- **Internal vs. external threats.** Many security risk management systems focus on external threats. However, there is growing evidence of security threats to staff emanating from colleagues themselves. Aid workers who identify as lesbian, gay, bisexual, trans, queer/questioning, intersex plus (LGBTQI+) or as persons with a disability have stated that they are more concerned about internal threats than external ones.[9] Internal threats can include verbal and physical abuse, blackmail, harassment, discrimination and violence. Behaviours and environments contribute to hostile work cultures, and minor instances of hostility can develop into more severe forms of aggression. This escalation is often described as a 'continuum' or 'pyramid' of violence, where seemingly trivial incidents of harassment, incivility and exclusion not only

8 For a detailed illustration of this point, see Hoppe, K. (2017) *Where is safe?* TEDxBristol, 19 December (www.youtube.com/watch?v=Q9RxE9p9T3w).

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

become normalised but also set the stage for more serious abuse.[10] A culture that tolerates these minor aggressions increases the risk of these incidents escalating.

- **Staff categorisation.** A lot of emphasis in security plans has historically been placed on how staff are categorised within an organisation (e.g. national, international, resident or mobile). This can prove problematic as categorisation can be complex and may not account for important identity factors, such as dual citizenship, and whether 'national staff' are local to the area or not. This may also lead to incorrect assumptions about staff members' vulnerability to threats, and their knowledge of security contexts. It is often more effective to consider each individual's specific situation as well as the contextual needs and circumstances, rather than relying on broad classifications. Efforts to localise positions within international organisations must also be carefully considered against personal risk profiles and individual strengths and vulnerabilities.

▶ *For a more detailed discussion on staffing, see Chapter 5.1 on human resources.*

1.2.2 A person-centred approach

Historically, where security risk management systems have considered identity, this has focused primarily on issues related to gender, ethnicity and nationality, and often in an ad hoc manner. Over the years, this focus has expanded to include a wider range of identity characteristics.[11] This shift, driven by the need for a more inclusive security culture in the sector, led to the introduction of a person-centred approach to security risk management. This incorporates identity-based considerations and places individuals at the centre of security risk management activities. In practice, it involves recognising profile-specific risks due to the intersection of individual characteristics (intersectional identity) and behaviour, organisational factors and the context in which staff are working (both in the physical and digital spheres) (see Figure 2).

10 To learn more about the pyramid of violence, see EISF (2019) *Managing sexual violence against aid workers: Prevention, preparedness, response and aftercare* (https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/).

11 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).

Figure 2 A person-centred approach to security risks

Adapted from Arthur, T. and Moutard, L. (2022) *Toward inclusive security risk management: the impact of 'race', ethnicity and nationality on aid workers' security*. GISF (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

A person-centred approach to security risk management involves tailoring security measures to the specific needs and vulnerabilities of individual aid workers, rather than applying a one-size-fits-all model. It promotes equitable risk mitigation by considering the unique intersectional identities of aid workers.

Security and decolonisation efforts

In addition to enhancing security risk management, a person-centred approach to security can support the 'decolonisation' efforts being made by an increasing number of international organisations. Security staff can promote both objectives by engaging in the following practical actions.

- **Critical reflection.** Engaging in critical reflection on the historical and structural factors that influence security risks. Historical, contextual and structural inequalities can place particular individuals at greater risk than others, often without the commensurate security measures to protect them, the power to ensure their security needs are heard and met or the ability to genuinely consent to the risks they are exposed to.
- **Inclusive dialogue.** Fostering inclusive dialogue to understand diverse perspectives and experiences. This can help identify and address biases and inequalities in security practices and ensure that security risk management measures are inclusive. It includes being open to knowledge and good practice from individuals with diverse perspectives.
- **Equitable support.** Ensuring that resources are allocated equitably to support the security of all staff, regardless of their identity. This can mean adopting a person-centred approach to security and may involve redistributing resources to address disparities and ensuring equitable security support for marginalised or under-represented groups. The question of equitable support is also relevant when working with partners (*see Chapter 3.5 for a more detailed discussion*).
- **Empowerment and representation.** Promoting the representation of marginalised and under-represented staff in decision-making processes, including risk assessments and security planning. Security staff can play an important role in facilitating discussions and providing expertise and experience that can translate into more inclusive organisational frameworks. This can also include striving for greater diversity in security professionals at all levels within an organisation. Leadership teams can also be vocal about how diversity in identities and experiences is an asset in humanitarian operations, and security risk management efforts.

1.2.3 Good practice considerations

Organisational culture

Local cultural norms and taboos can make discussions around specific identity characteristics, such as ethnicity and sexual orientation, especially challenging. This cultural resistance can hinder the implementation of inclusive security risk management efforts, which can require open and sensitive discussions about these topics. Some organisational leaders may also worry that investigating the experiences of staff with minority profiles could draw attention to potential organisational shortcomings, risking reputational harm.

Creating and enforcing policies that support a person-centred approach systematically requires institutional commitment and support. This can include developing comprehensive guidelines, allocating resources for training, and ensuring that these policies are integrated into the broader organisational culture. Many organisations still struggle to consistently incorporate inclusive considerations and language in their policies, training and daily communications.

Leadership teams can focus on empowering security focal points to adopt a person-centred lens through all elements of their work, including collaboratively developing an inclusive security risk management framework. Security staff can play an important role in fostering a culture of confidentiality, collaboration, inclusivity and trust, and they should strive to be viewed within the organisation as approachable and reliable. Some organisations have security focal points in each office who are female and/or locals to the area, to improve reporting on sensitive issues.

A key challenge is determining the balance between individual responsibility and organisational duty of care. It is advisable for leadership teams to thoroughly research and understand their responsibilities in fulfilling this duty, particularly when considering the diverse profiles of their staff. Failure to adequately address identity-based risks could result in a failure to discharge this duty of care, especially as the vast majority of the aid workforce is made up of individuals from diverse backgrounds. A security risk management system that accounts for the diverse security needs of staff not only helps to mitigate these risks, but can also improve staff wellbeing and retention and programme outcomes. Organisations should be clear about the level of support they provide for managing identity-based risks, while also encouraging individuals to seek guidance and support for specific needs.

Addressing discrimination

Concerns about discrimination are a significant obstacle to organisations addressing identity-based risks. Organisations do not want to be seen as invading staff privacy or making employment decisions based on personal characteristics, and they may rightly worry about the legal implications of doing so. This has led some organisations to adopt a 'don't ask, don't tell' approach, where security decisions based on identity aspects are not transparently communicated or openly discussed. However, treating all staff members as if they had a single, common risk profile can lead to inadequate protection, increased vulnerabilities and even greater organisational risks. Recent research has found that aid workers would like to see identity-based risks more transparently and openly addressed in security measures.[12]

In some circumstances and contexts, people with certain profiles may need to follow distinct security measures or require additional security support. Whether the imposed measures and resources are justifiable will depend on whether these actions are legitimate and proportionate to the risk, or if less drastic alternatives exist. All decisions should aim to be based on documented evidence rather than individual assumptions or perceptions.[13] In effect, what would make these measures unjustifiable is if they were arbitrary and the differences led to unjust treatment or inequality.

To understand this better, it is helpful to distinguish between equitable treatment and equal treatment. Equal treatment implies providing the same resources and measures to everyone, regardless of their circumstances. However, this approach can overlook specific vulnerabilities and fail to provide adequate protection. Equitable treatment involves providing tailored resources and measures to ensure that all individuals have the same level of security and support, accounting for their specific needs and risks. The aim is to ensure that the resultant level of risk is acceptable for everyone. This approach is not discriminatory but rather a necessary adjustment to address real and varied threats effectively.

Ensuring that measures are not discriminatory and are more readily accepted by staff can be facilitated through:

- **Collaborative policy and practice development.** Involving diverse staff in the development and review of security policies and practices ensures

12 EISF (2018).

13 For a more detailed discussion of legal anti-discrimination considerations, see EISF (2018), Chapter 2: Legal duty of care and anti-discrimination.

that the organisation's approach reflects a wide range of perspectives and addresses the concerns and specific risks faced by different identity groups. Organisations can establish consultative spaces, advisory committees or working groups that include representatives from various identity groups to contribute to the development or review of security measures.

- **Explicit and timely communication.** Informing staff of the risks and clearly communicating the reasons for tailored security measures in a timely manner (e.g. before travel or during recruitment) helps ensure that everyone understands the necessity and fairness of these measures.
- **Feedback mechanisms.** Establishing channels for staff to provide feedback on security measures and regularly soliciting and acting on feedback helps identify any issues of perceived discrimination and allows for continuous adaptation and improvement of security practices as environments and risks change.

Inclusive security systems, policies and practices

Introducing a new way of working can be daunting. Security staff often operate under tight deadlines and heavy workloads, making it difficult to allocate time for considering a new approach and adopting person-centred ways of working. Security staff may also feel unable to engage in identity-based risk conversations due to a lack of expertise. Despite these challenges, some organisations have made significant strides in adopting a person-centred approach to security, often driven from the top, with senior leadership taking the initial measures, including encouraging and empowering their staff to adopt this approach. For some organisations, this has meant consultations with staff to understand the identity-based risks they face; for others, it has involved hiring more diverse security teams, and for one international organisation it has involved assessing all aspects of its security systems to identify ways they could be more inclusive (see case example box below).

Many efforts have started small, with targeted shifts in particular areas that then snowballed. Initiating a person-centred approach does not necessarily require a significant investment of money or time, but can start with a shift in perspective, for example by security staff simply asking how a situation or programme may impact the security of colleagues with different profiles and needs.

Case example: Adopting a systematic person-centred approach to security

One international organisation's global security team initiated a project to establish a guiding framework for a person-centred approach to security risk management. The primary objective of the project was to identify diversity and inclusion gaps in security risk management (through research and staff consultations) and then provide practical recommendations.

Most staff consulted for the project felt that personal profiles were an important factor in determining the level and type of security risks they faced, but that the organisation, and particularly managers, needed to do more to address profile-specific risks.

The research found the main profile-related security challenges to be lack of access to relevant information, internal discrimination/unequal treatment and external prejudice/hostility in the local environment. Factors making staff feel more secure included open communication on security-related issues from the management team, clear written security policies and procedures and mechanisms for reporting incidents or any relevant information to better understand the overall working environment, as well as for addressing complaints.

The research indicated the need for a more systematic and inclusive approach to security risk management, as well as a more proactive and inclusive management culture. Following the project, the organisation took steps to implement the recommendations identified, which required the input of several different internal workstreams and decision-makers. Given the organisation-wide changes required, it was important to ensure implementation was the shared responsibility of various stakeholders, including security, human resources, and other departments involved in training, policy development and data collection.

Diversity considerations can be factored in across the security risk management framework.

- **Inclusive risk assessments.** A comprehensive risk assessment process integrating individual (intersectional identity and behaviours), organisational and external risk factors, considering both internal and external threats and their inter-relationships. Another factor to consider may be time (as certain periods, such as during elections, may be more insecure than others). Smaller organisations, or those with less staff movement, may be better able to carry out individualised risk assessments for each staff member when they join the organisation, start a new project or travel (this is an approach taken, for example, by some human rights organisations). Larger organisations that would struggle with this may find it helpful to ensure that risk assessments involve the greatest diversity of staff, to ensure that a range of perspectives are incorporated, and to provide staff with the tools and training to carry out their own individual risk assessments and seek guidance when needed.
- **Security plans and response measures.** Ensuring that risk mitigation measures, security plans and response mechanisms consider the diverse needs of staff. This can mean, for example, ensuring that staff with disabilities are adequately considered in site security and evacuation plans, or that the nationalities of staff are considered in contingency plans (e.g. evacuating some nationalities to a particular country may place them at heightened risk). For resident staff – nationals and foreign nationals alike – it can be advisable to incorporate family considerations into contingency plans. This can be achieved through the collaborative approaches detailed in various parts of this chapter.[14]
- **Security tools.** Incorporating questions and information around identity-based risks into existing security tools. This can include options for selecting identity-based qualifiers in incident report forms to allow for better incident analysis, which can help determine whether incidents may be the result of discrimination, homophobia, ethnically motivated targeting or other factors.
- **Guidance.** Providing guidance so that staff who do not wish to disclose personal identity concerns have access to information to make informed security decisions. The key here is for information about profile-specific risks to be shared systematically with all staff, regardless of their personal profiles. This can include incorporating identity-based risk information in security documents shared with staff, and providing staff with focal points they can speak to on a confidential and one-to-one basis. Organisations can collaborate with specialist groups and initiatives to incorporate their expertise and resources into internal guidance. This could include working with organisations that address gender-based violence or support LGBTQI+ individuals. Staff may have their own

14 For detailed examples on inclusive risk mitigation measures see EISF (2018).

resources and guidance, but how an organisation makes information available, and what type of feedback loop is provided, can make a big difference in how staff interact with the guidance they are given. This can also improve the content of guidance developed and maintained by the organisation.

- **Security culture.** Building a positive and inclusive organisational security culture by communicating with staff about identity-based risks, destigmatising discussions and tackling 'myths' around personal vulnerability in group settings, such as briefings and training. This type of communication can empower staff to voice concerns and make more informed security decisions for themselves and others.
- **Security staff composition.** Recruiting diverse security staff. More organisations are aiming for greater diversity in staff generally, but also in security positions. The identity of security focal points can significantly influence staff perceptions of – and engagement with – security measures.[15] In practice, this can mean being mindful of job requirements. For example, in countries where women are barred from police or military roles, making this experience a requirement for security positions will exclude national female candidates.

Roles and personal risk profiles

In some contexts, certain visitors may have elevated risk profiles due to their visibility or role (for example, VIP visitors). These individuals may include organisational leaders, experts, donors, government officials and auditors, whose presence can attract unwanted attention or aggression (within and outside an organisation). The targeting of such individuals can have severe repercussions for the individual's security, and for the broader organisation. It may also increase the security risks to staff, raising important questions about the criticality of such visits. If the visit warrants the risk entailed to the visitor and other staff, organisations can implement appropriate security measures, which may include discreet security details, secure accommodation, special travel protocols, information security measures (such as not disclosing location information publicly) and contingency planning for emergencies. For organisations where VIP visits are common, regular training for these individuals and those who interact with them on personal security awareness and behaviour in high-risk environments is beneficial.

15 To learn more, see: GISF and Humanitarian Outcomes (2024).

Guidance on identity-based risks

Staff have a right to privacy, which means that organisations cannot force them to disclose information about their personal profiles they do not feel comfortable sharing. By providing general guidance on identity-based risks, organisations avoid pressuring staff to disclose sensitive information or singling out staff directly due to assumptions around their identity. This also contributes to building a security culture that allows each person to raise questions and reflect on their own security needs.

The following sample questions can support organisations in deciding what guidance to provide:

- What is the make-up of staff? Aggregated and anonymised information from human resources (HR) can help with this. Using this data alongside contextual factors, which staff profiles may require additional guidance?
- Do staff understand the organisation's duty of care towards them? Is there any specific area where they need more information, and could this be addressed through additional guidance?
- What resources do staff have access to relating to identity-based risks (external and internal)? How can the organisation help them access this information more easily?
- Are staff able to comfortably and confidentially access resources pertaining to identity-based risks?
- Is there a focal point staff can confidentially approach to discuss their concerns?

One organisation has ensured that, as part of its travel procedures, links are provided to external and internal resources for risks and guidance relevant for LGBTQI+ staff. The organisation's intranet site also has a dedicated page providing guidance.

Making broader organisational practices inclusive

It can be helpful to apply a person-centred lens to broader organisational practices that can affect staff security.

- **System reviews.** Conducting organisational reviews that assess whether all staff have adequate access to support and resources (including on security), no matter their personal profile and addressing any identified barriers or structural inequalities. In any organisation, especially international ones, it is advisable to adapt communication and interactions to the target audience. A simple example is ensuring that staff can access relevant communications in their first language. In many international organisations, international and national staff may have access to different levels of support, including insurance. In some circumstances these additional support services are justifiable and needed, but this can also indicate failures in equity across all staff. It is also important to note that these distinctions may not be due to bias or inattention, but a result of factors outside the organisation's control, such as legal barriers to the evacuation of national staff and limitations to insurance policies.
- **General recruitment and deployment.** Integrating identity-based security considerations into recruitment procedures, and, if appropriate, in discussions with staff prior to new assignments.[16] This can, in practice, mean being open to different experiences and ensuring that job requirements are not unduly exclusionary of particular profiles (see box below).

16 For a more in-depth discussion of consideration of identity-based risks in recruitment, see EISF (2018).

Identity issues in recruitment and deployment

Recruitment or deployment of staff in the humanitarian sector is more complex than in many other areas of work. Some individuals may be at heightened risk in new locations or roles due to their personal risk profiles. It is advisable to encourage discussion whenever possible rather than to place a blanket ban on specific profiles. This said, in some cases it may be advisable to state in the job description that particular roles are not open to specific identity profiles due to the security situation. The legality of this type of indirect discrimination depends on the country; measures should always aim to be justifiable, proportionate and legitimate. An example would be not recruiting men to work in a women's refuge or shelter.

Involving security focal points in recruitment and deployment, and being clear in job descriptions and during interviews about the heightened risks faced by particular profiles, ensures that these concerns are discussed and decided openly in conjunction with affected staff.

Training

Addressing identity-based risks in security training can improve outcomes for all staff, from how team members can support colleagues with a disability in the event of an emergency to maintaining the confidentiality of a colleague's sexual orientation following a security incident – particularly if disclosure of this information could present a security risk for the staff member or the organisation.

Although trainers have experienced resistance to covering these topics, addressing diversity in these courses can be an opportunity for dialogue and to share the lived experiences of under-represented profiles among team members, which otherwise might never have been heard or understood by colleagues. While trainers cannot be expected to have every answer to every question regarding an identity-based risk, they can create a space for participants to examine questions for themselves and their individual profiles, while leveraging the common experiences of others.

The identity of the trainer can also play a role in a training participant's level of comfort to engage in questions surrounding their individual profiles. While

increasing the number of trainers from under-represented groups is core, so too is the ability of all trainers, no matter their profile, to foster an environment where concerns can be welcomed and safely considered.

▶ *For more details on training and inclusivity considerations, see Chapter 5.2.*

Targeted training considerations

Beyond ensuring that security training is more considerate of diverse risk profiles, organisations can also provide staff, including security staff, with training on unconscious bias, power, privilege, intersectionality and being empowered bystanders, to name a few. Some organisations have woven these aspects into their existing security training. These areas of learning can help to build awareness of the risks faced by different identity groups and promote a culture of inclusivity and respect. When staff understand the rationale behind tailored security measures, they are more likely to see them as fair and necessary, reducing resistance and perceptions of discrimination. For security staff, training in these areas can deconstruct assumptions around personal risk profiles, help build empathy and promote practical skills for managing identity-based risks.

It is advisable to train security staff and other relevant colleagues (such as HR) on how to adopt a person-centred approach, for example how to conduct an inclusive security risk assessment. This ensures that responsible staff are able to address identity-based risks, and are comfortable discussing these issues with staff.

Case example: UN Operational Safeguarding

The UN Department of Safety and Security (UNDSS) has developed a concept of 'operational safeguarding', which applies to policies, procedures, measures and training implemented within the UN to protect its staff, assets and operations from interpersonal harm. It focuses on both internal and external threats to staff and recognises that efforts to tackle internal threats against UN staff go hand-in-hand with efforts to address sexual exploitation and abuse by UN personnel.

Operational safeguarding promotes a person-centred approach to security through the implementation of inclusive security tools and by focusing on perpetrators (known and unknown), their allies, the operating environment and the personal and situational vulnerabilities of potential targets.

Key elements of this approach include:

- Recognising that behaviours and environments can lead to abuse of power, and that minor instances of hostility can escalate into more serious forms of harm (the 'pyramid of violence'). Tolerating harassment, incivility and exclusion increases the likelihood of more serious incidents, including sexual assault.
- Recognising that all forms of interpersonal aggression have relevance to security staff as they are a serious cross-cutting problem, requiring collaboration between all departments that deal with staff.
- Ensuring that every staff member is informed about all potential threats, not just those that seem relevant to each individual. By equipping all personnel with the knowledge and tools to mitigate risks universally, the UN aims to enhance security for everyone. Essentially, collective security is achieved only when each member is secure – no one is truly safe until everyone is safe.
- Promoting a UN Upstander approach, encouraging trained staff to become empowered bystanders in the event of an incident and promote operational safeguarding in the course of their work.

The UN has rolled out blended training on operational safeguarding. The interactive training aims to raise awareness among staff on how to implement this approach and upskill personnel as 'UN Upstanders'. In addition to raising awareness and empowering staff, the training aims to be a significant deterrent to would-be perpetrators.

Further information

Research and discussion

Arthur, T. and Moutard, L. (2022) *Toward inclusive security: The impact of 'race', ethnicity, and nationality on aid workers' security.* GISF (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

EISF (2018) *Managing the security of aid workers with diverse profiles* (www.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* (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Hoppe, K. (2017) *Where is safe?* TEDxBristol (www.ted.com/talks/kelsey_hoppe_where_is_safe/details).

Guidance and tools

Bond (2022) *Becoming locally led as an anti-racist practice: a guide to support INGOs* (www.bond.org.uk/resources/becoming-locally-led-as-an-anti-racist-practice-a-guide/).

EISF (2019a) *Managing sexual violence against aid workers: Prevention, preparedness, response and aftercare* (https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/).

EISF (2019b) *Beyond the tick box: Developing a person-centred and inclusive approach to security risk management*. 16 December (http://gisf.ngo/blogs/beyond-the-tick-box-developing-a-person-centred-and-inclusive-approach-to-security-risk-management/).

GISF (2021) *HNPW | A person-centred approach to security risk management | Resources* (https://gisf.ngo/resource/hnpw-a-person-centred-approach-to-security-risk-management-resources/).

GISF (n.d.) *2. Inclusive security.* NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/inclusive-security/).

ICRC (2021) '3.3. Is everyone equally at risk?' in *SAFE: Security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Persaud, C. (2012) *Gender and security: Guidelines for mainstreaming gender in security risk management*. EISF (https://gisf.ngo/resource/gender-and-security/).

RedR UK and EISF (2016) *Workshop report: Inclusion and security of LGBTI aid workers* (https://gisf.ngo/resource/report-inclusion-and-security-of-lgbti-aid-workers-workshop-22012016/).

United Nations (n.d.) *Gender & security* (www.un.org/en/safety-and-security/gender-and-security).

2 The ecosystems of security risk management

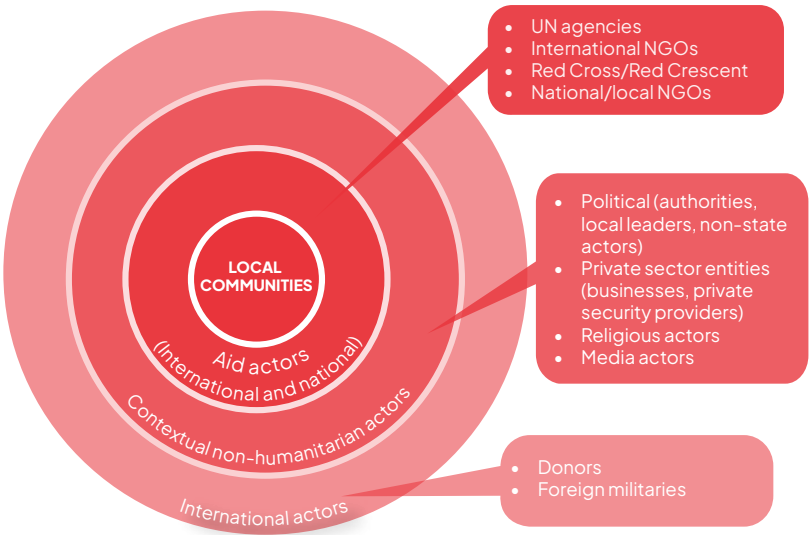
2.1 Security collaboration and networks

Humanitarian organisations do not operate in a vacuum. On a daily basis, they interact with friendly, unfriendly and neutral actors at various levels. The number of interlocutors has only grown in recent years, as more humanitarian actors, private sector entities and non-state armed groups operate in the same spaces. This chapter outlines the main actors and relationships influencing humanitarian security risk management and explores how security staff can deepen their understanding and improve coordination and collaboration to enhance security while advancing humanitarian objectives.

2.1.1 Understanding the external ecosystem

When a humanitarian crisis occurs, various local, national – and often international – actors respond with interventions to meet the needs of affected people and communities. These humanitarian actors, both formal and informal, are diverse, each with their own legal status, objectives and policies. In this complex, often crowded, humanitarian space, coordination is imperative to pursue common humanitarian goals. Outside the humanitarian sphere, organisations navigate an even wider ecosystem of public and private organisations, political entities, military groups and financial institutions (Figure 3).

Figure 3 The external ecosystem



Each of these actors can present potential threats or opportunities for security risk management.

2.1.2 Security collaboration and coordination

Interagency security collaboration

As security risk management has developed within humanitarian organisations, so too have the structures, means and practices for organisations in the same operating environment to cooperate with each other on security. Effective collaboration among organisations enables each participant to significantly enhance the effectiveness of their own security risk management systems in the following ways.

- **A better alert system.** By sharing information with each other, organisations receive a fuller picture of actual or possible security threats or alerts in their environment, which improves response planning and increases the chances of avoiding an incident.

- **Better risk assessment.** A centralised compilation of all security incidents and near-misses involving aid workers in a given operating environment is a better basis for a security risk assessment than a single organisation's partial record.
- **Cost-effective additional capacity.** Rather than each organisation individually carrying the costs of additional inputs, these can be brought in on a cost-shared basis. For example, the costs of specialist consultations or a security training course can be shared by several organisations.
- **Collective advocacy and negotiation with authorities.** Rather than engaging individually on issues pertaining to security, organisations can potentially make a stronger case to governments and other stakeholders as a group.
- **Advocacy for funding with donors.** If the security situation deteriorates and several organisations conclude that they need extra financial resources for additional mitigating measures, they may be able to make a more effective case with donors collectively.
- **Direct assistance and gap-filling.** If one organisation has the capacity to host additional staff during a lockdown, or transport to relocate or evacuate staff when others do not, prior coordination and planning can ensure effective use of these resources.
- **Common service provision.** Established coordination mechanisms can use economies of scale to provide services such as centralised security information and analysis and training.
- **Sharing good practice.** Organisations can learn from each other when they collaborate and share information, advice and good practice on how to manage risks in a specific area of operation.
- **Managing interdependent risks.** The security measures (or lack of them) of any one organisation can have repercussions for others. For example, if one organisation uses armed security escorts or pays 'facilitation fees' at checkpoints, this can create problems for those who do not. Cooperation can identify and address these inconsistencies.

Interagency security coordination mechanisms

Interagency security coordination mechanisms exist at global, regional, country and area levels. They can be formal and informal.[17]

17 For more detailed information on security collaboration, see GISF (2022) *NGO security collaboration guide* (https://gisf.ngo/long-read/ngo-security-collaboration-guide/).

Formal mechanisms for NGOs – such as the International NGO Safety Organisation (INSO), USAID's Partner Liaison Security Operation (PLSO) and the security arms of NGO coordinating bodies – may provide analytical products, such as regular security reports and security trend analysis. Such mechanisms also provide space for discussion, and may organise forums and security training opportunities.

NGO security bodies often interface with UN agencies on security matters through the UN Humanitarian Country Team and the UNDSS. Coordination and collaboration between NGOs and UN agencies can help with conducting joint access assessments and developing secure access strategies, coordinating contingency planning for emergencies, and managing advocacy and liaison with government authorities, UN bodies, military forces and private security actors.

Where no formal coordination body exists, security focal points from different organisations will often establish an informal network to share information, alerts and advice, often using online or SMS-based platforms. Participation in these groups tends to be voluntary and ad hoc, based on individuals as opposed to organisation representation.[18] At the time of writing, informal networks exist for regional security staff in West Africa and Latin America and the Caribbean.

Historically, security coordination mechanisms in humanitarian contexts have been created by – and centre on – international organisations, with local and national organisations less represented. This is slowly being addressed, as the value of coordination is increasingly understood to rise with the number of actors participating, especially those that bring deep contextual knowledge and diverse sources of information.

At the global level, coordination between NGOs – and between NGOs and the UN – has also advanced in recent years. GISF is an interagency platform for sharing information and good practice related to humanitarian security risk management. GISF serves as a hub for expertise, developing guidance and conducting original research. INSO also plays a role at the global level, providing analysis, training products and security data. The International NGO Safety & Security Association (INSSA) is a membership organisation offering professional certification for country- and regional-level security risk managers specific to the aid sector. Global working groups focus on particular topics related to security risk management, such as safeguarding and humanitarian access.

18 For a more in-depth discussion, see 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).

Several countries have security coordination networks for organisations with head offices there, for example the Danish Interagency Security Network and the UK NGO Security Focal Point Group. Security coordination can also be a component of a broader coordination mechanism, such as InterAction in the US and La Coordinadora in Spain. As the humanitarian security field has developed, there are also more specialist security roles and a growing number of coordination platforms specifically for these professionals.

Saving Lives Together

Since 2001, security collaboration and coordination between the UN and international NGOs has been structured by a written framework known today as Saving Lives Together (SLT).[19] SLT has gone through several iterations over the years, but from the beginning has aimed to provide a common understanding of the opportunities for NGOs, UN agencies and the International Red Cross and Red Crescent Movement to work together in the face of common security challenges. Its goal is to enhance partners' ability to make informed decisions and manage risks through shared information and resources.

Participants in SLT commit to six main objectives/requirements:

- establish security coordination arrangements and forums;
- share relevant security information;
- cooperate on security training;
- cooperate on operational and logistics arrangements, where feasible;
- identify resource requirements for enhancing security coordination between the UN, international NGOs and international organisations, and advocate for funding; and
- consult on common ground rules on humanitarian action.

The SLT Oversight Committee, co-chaired by UNDSS and international NGO representatives, ensures effective implementation and coordination. All international NGOs with operations in a country can participate, with no fees, though some services may have cost recovery. While local organisations cannot attain SLT partnership status, they can benefit through existing NGO security networks.[20]

19 SLT's first incarnation was a memorandum of understanding (MoU) called the Menu of Options, established by the Inter-Agency Standing Committee (IASC) with the UN Security Coordinator (UNSECOORD, the forerunner of UNDSS).

20 To learn more about SLT, see https://gisf.ngo/themes/coordination-for-hsrm/saving-lives-together/.

Although the SLT framework has been revised and relaunched, operationalising it at the country level has been challenging, limited and slow. Awareness of the framework's existence and purpose is still limited among both NGOs and UN staff, and in some areas a lack of trust between the UN and NGO communities further hinders progress.[21] Even so, SLT has met with success in contexts where there is strong and effective leadership in UNDSS and the humanitarian country teams, as well as coordinated and proactive outreach by NGOs.

Private security providers

Private commercial security has grown significantly over the past two decades. The term 'private security provider' (PSP) can refer to both officially registered companies and unregistered groups, such as hired militias, that provide similar services. The most common use of private firms for security by humanitarian organisations is the contracting of private guarding companies to secure premises and programme facilities.

PSPs offer a wide range of services, including static protection (securing offices and residences), mobile protection (escorts), close protection (bodyguards), threat assessments, risk analysis, security audits, training, consultancy, critical incident management, crisis support, logistics (such as cash-in-transit security) and equipment provision.

Although the use of armed protection by PSPs is uncommon, humanitarian organisations have at times engaged them for unarmed guarding and other support services, including analytical work. Decisions to hire PSPs often rely on assumptions about their expertise, efficiency and cost-effectiveness – but these assumptions should be carefully examined. While outsourcing security might seem cheaper initially, hidden costs could include a failure to develop in-house skills, potential reputational damage, legal liabilities and the risk of dependence on a deterrence-based security approach that could become more expensive over time.

When employing PSPs, organisations must carefully consider who they hire and how they will be employed. Guards at offices, guesthouses and warehouses often serve as the public face of the organisation, making them essential to overall security beyond their basic watch duties. It is also crucial to assess potential links between PSPs and military or political actors as they may be connected with state security forces, police or individuals with a history of illegal or abusive behaviour, including human rights violations. Evaluating a PSP's wider practices can be challenging due to confidentiality and the complex ownership structures of some companies.

21 To learn more about these challenges, see GISF and Humanitarian Outcomes (2024).

A helpful resource is the International Code of Conduct Association (ICoCA), which was established following the Montreux Document on legal obligations and good practice for private military and security companies, and which provides standards for good practice among PSPs. ICoCA acts as the governing and oversight body for the International Code of Conduct for PSPs, which aims to ensure respect for human rights, compliance with international law, and accountability for misconduct. Determining whether a PSP is registered with ICoCA can form a valuable part of the due diligence process as the Association promotes good governance, human rights, international humanitarian law and high professional standards within the private security industry.

When considering the use of PSPs, several strategic, operational and legal factors may need to be taken into account. External expertise, such as guidance from bodies like ICoCA, may also be useful, especially if internal capacity is limited. Organisations might assess whether engaging a PSP aligns with their mandate and security strategy, whether it reduces long-term risks, and how it could affect their reputation, both locally and internationally, as well as evaluating their capacity to manage such providers. It is also important to determine whether the use of PSPs might set a precedent or contribute to market inflation, potentially affecting local communities and other humanitarian actors. How PSPs may enhance public security and ensuring compliance with relevant government regulations are also important considerations.

During the background check and hiring process, it can be useful to implement robust due diligence procedures, maintain clear contract templates and keep detailed performance records. Verifying that a PSP operates with a clear code of conduct, has well-trained personnel with defined rules of engagement and adheres to legal standards may ensure reliability. Considering the provider's ethical commitments, training programmes and anti-corruption measures is also important. Contracts could specify performance monitoring and compliance requirements. It is strongly recommended to ensure that PSPs have internal mechanisms for addressing misconduct and abuses.

Ongoing oversight and monitoring of PSPs may help organisations ensure that providers uphold high standards and protect both their interests and those of the public. It can also help to mitigate hidden risks, such as becoming overly reliant on external providers, which might impact an organisation's ability to build internal expertise in security risk management.[22]

22 For more good practice recommendations, see Davis, J. et al. (2020) 'Module 14, Contracting private security providers' in *Security to go: a risk management toolkit for humanitarian aid agencies,* 4th edition. GISF (https://gisf.ngo/resource/contracting-private-security-providers/).

► *For a discussion on the use of armed escorts, see Chapter 4.2.*

2.1.3 Engaging with the authorities

The government of a crisis-affected country has certain responsibilities towards the security and protection of aid organisations, and these are reflected in national legislation, international humanitarian law and UN host country agreements. In principle, these include the following.

- **Ensuring safety and security.** As the primary 'duty bearer', governments are responsible for maintaining law and order, ensuring a safe environment and protecting all individuals and entities from violence and crime.
- **Facilitating safe access.** Governments are responsible for helping enable humanitarian access to areas where aid is needed, ensuring that aid workers can operate without undue restriction, interference or threat. This includes provision of visas, permits and licences.
- **Providing a legal and regulatory framework.** Establishing and enforcing laws that protect aid organisations from harassment, attacks or other threats to personnel, operations and assets.
- **Coordination and communication.** Governments are expected to coordinate with aid organisations, sharing information on security threats, risks or incidents, and to work collaboratively on safety measures.
- **Investigating and prosecuting the perpetrators of attacks.** In case of attacks or incidents involving aid organisations, the government is responsible for investigating, apprehending and prosecuting perpetrators to ensure accountability.
- **Respecting humanitarian principles.** The neutrality, independence and impartiality of humanitarian operations should be respected, avoiding actions that could compromise the principles or damage the perceptions of aid organisations in contested environments.

In reality, the government may be more or less capable of providing a safe environment and may be a party to the conflict that created the humanitarian crisis. In rare cases, such as the cross-border humanitarian aid deliveries to Syria during the Syrian civil war sanctioned by the UN Security Council, and covert aid operations for Myanmar across the Thai border, organisations may operate without government agreement or engagement. Governments will also vary on the extent to which they lead, support or participate in the coordination of the

humanitarian response. At times, they may politicise, impede, attack or interfere with aid delivery. This may also be the case for foreign governments with military or other interests in the country in question.

For their part, aid organisations are obliged to consult and seek government approval and support for their presence, explaining the purpose and objectives of their activities, even when the government is a party to the conflict or actively impeding humanitarian efforts. Continuous exchange with the relevant government counterparts, including, at times, foreign authorities, is often vital to secure humanitarian action, and organisations can cultivate an ongoing relationship and rapport with government counterparts through regular liaison, meetings and courtesy visits.

At the same time, it is advisable for security staff to exercise caution when engaging with government counterparts, particularly in contexts where authorities may be hostile to aid efforts. Sometimes even using a term like 'security' can raise suspicion or invite scrutiny, potentially leading to restrictions on operations or heightened surveillance of the organisation. It helps to approach such engagements with sensitivity, clearly defining objectives to avoid misunderstandings while remaining vigilant to any attempts by the government to exploit the interaction for information-gathering or to undermine the organisation's activities. Working in coordination with other aid actors, through established collaboration networks, can facilitate these interactions.

When operating in crisis environments, humanitarian organisations may also need to liaise with sub-state actors, such as regional or local authorities. These actors, while not holding the same authority as national governments, often exert considerable influence over specific areas. Establishing a relationship with sub-state authorities can be crucial to securing humanitarian access, particularly in regions where the central government's reach is limited or where there is a need to liaise with several different de facto authorities. Clear communication of the organisation's humanitarian mandate, with an emphasis on neutrality and impartiality, can assist in mitigating tensions and fostering trust. Sub-state actors may have their own interests, which could impact the security and perception of aid efforts. Engaging in consistent dialogue and working in coordination with other aid actors, as well as trusted community leaders, can be beneficial.

Non-state armed actors

In conflict zones where non-state armed groups control territory, humanitarian organisations may need to establish dialogue to negotiate access and ensure the safety of their personnel. Non-state actors can differ significantly in their approach to humanitarian assistance, with some recognising and facilitating access, while others may be more hostile.

Engagement with such actors requires careful preparation, including an understanding of their motivations, political affiliations and relationships with other conflict parties, as well as local communities. Even day-to-day interactions can be challenging and, in addition to security risks, may create dilemmas regarding humanitarian principles and the organisation's own red lines. The Centre of Competence on Humanitarian Negotiation (CCHN) was established by the International Committee of the Red Cross (ICRC) and other organisations to provide support, coordination and capacity development for humanitarian negotiations, and can be an important resource.[i]

Before engaging in any dialogue with non-state armed actors, it is good practice for organisations to:

- Define the scope and objectives of the engagement.
- Analyse the specific context within which the dialogue is going to take place.
- Map out the different actors and understand the motives and interests (stated and hidden) of each actor.
- Understand the constituencies those actors represent (if any).
- Develop and agree a context-specific access engagement strategy.
- Agree on what is negotiable and what is not in terms of policies, principles, mandates and resources.
- Liaise/coordinate with other organisations working in the same space to understand their access standpoint and share lessons.
- Understand the legal status (locally and internationally) of these actors.

[i] See https://frontline-negotiations.org/home/discover/about-us/

► *For more on interacting with armed actors see Chapter 4.2 – Developing a security strategy.*

2.1.4 Engaging with militaries

Civil–military coordination

Militaries are often key actors in crisis contexts, either because they are engaged in armed conflict or because crisis-affected governments sometimes use national and international military forces and their assets to deliver relief in complex emergencies. In either scenario, coordination between the military and humanitarian actors is often vital to facilitate safe humanitarian action.

The principal entities for coordination between humanitarian organisations and militaries include the following.

- **UN Humanitarian Civil–Military Coordination (UN-CMCoord)** under the auspices of the UN Office for the Coordination of Humanitarian Affairs (OCHA). UN-CMCoord maintains dialogue with the military and other armed actors, including non-state armed groups, to promote interaction and cooperation between all actors in accordance with UN General Assembly Resolution 46/182 and existing civil–military coordination guidelines.
- **Civil–Military Operations Centres (CMOCs).** CMOCs are physical coordination centres established in conflict or disaster areas, where military, government and humanitarian organisations can share information and coordinate activities. They often function as a hub for communication and planning.
- **Humanitarian access working groups.** Initiated by OCHA, humanitarian organisations have collaborated in insecure and hard-to-access environments through humanitarian access working groups. These groups can serve as an entry point for dialogue with military actors, allowing humanitarian organisations to communicate their priorities, negotiate safe passage and advocate for adherence to humanitarian principles.

► *For more on access working groups and negotiations, see Chapter 3.2 – Access and security.*

It is important to note that the specific coordination mechanisms used may vary depending on the context and nature of the crisis. The UN-CMCoord framework provides flexibility in adapting coordination strategies ranging from cooperation

to coexistence, based on the specific situation. Liaison arrangements and common training play a crucial role in facilitating effective coordination between humanitarian and military actors. The *UN-CMCoord Field Handbook* outlines various coordination elements and tasks, including establishing dialogue, information sharing and monitoring military activities to ensure they do not negatively impact humanitarian action.[23]

Civil–military coordination activities can be especially fraught in conflict settings where interaction with military actors may be seen to compromise the neutrality, impartiality and operational independence of humanitarian actors. In such situations, humanitarian organisations will often try to maintain an operational distance and avoid overly relying on military assets and services for protection and logistical support.

Humanitarian notification system

The Humanitarian Notification System for Deconfliction (HNS4D) mechanism aims to enhance the security of humanitarian operations by notifying military actors about the locations of humanitarian facilities, movements and activities in conflict zones. Its objective is to minimise the risk of accidental attacks on humanitarian personnel and infrastructure by ensuring that military forces are aware of these protected sites.

HNS4D requires organisations to submit detailed information about their facilities, staff and planned movements to an intermediary, usually OCHA. This submission often includes Global Postioning System (GPS) coordinates, descriptions of the facilities and the nature of their activities. OCHA then consolidates this information and shares it with relevant military actors to ensure they have updated and accurate data on humanitarian operations in the area. The process aims to provide a layer of protection, with regular updates to maintain the accuracy of the information as operations evolve.

There have been instances where humanitarian organisations have lost confidence in the HNS4D due to repeated failures and lack of assurances from military counterparts. In Syria, Afghanistan and Gaza, international militaries bombed facilities operated by NGOs, even when humanitarian organisations repeatedly provided information and coordinates for these locations.

23 UN-CMCoord (2018) *UN-CMCoord field handbook.* Version 2.0. OCHA (https://gisf.ngo/wp-content/uploads/2021/11/E-Version-UNCMCoord-Field-Handbook-2.0-2018.pdf).

A realistic understanding of HNS4D's capabilities and limitations should guide organisations' decisions on engagement.[24]

2.1.5 Other non-humanitarian actors

A wide range of other actors may also be present, including businesses, local financial institutions and community groups, who can provide logistical and operational support. Development actors, local civil society organisations and human rights groups often have long-term commitments in many areas and can provide valuable insights and support. By engaging with these entities, humanitarians can also ensure that their interventions are complementary to existing efforts, avoiding disruption to ongoing work by these groups and fostering a more sustainable, locally grounded response.

Further information

Research and discussion

Bebbington, C. et al. (2022) *Reviewing guidance and perspectives on humanitarian notification systems for deconfliction*. Center for Human Rights and Humanitarian Studies, Watson Institute for International and Public Affairs, Brown University and Humanitarian Response Program, College of Maritime Operational Warfare, US Naval War College (https://watson.brown.edu/chrhs/files/chrhs/imce/research/2022%20HNS4D%20Research%20Paper%20-%20CHRHS%20%26%20HRP.pdf).

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).

GISF (2023) 'Humanitarian notification systems: Unpacking the complexities and possibilities (No. 3)' [Podcast] in *Evolving NGO security risk management* (https://gisf.ngo/resource/evolving-ngo-security-risk-management-ep3-humanitarian-notification-systems-unpacking-the-complexities-and-possibilities-gisf-podcast/).

UN OCHA (2021) *Concept note on humanitarian notification in support of access and protection in Syria* (https://reliefweb.int/report/syrian-arab-republic/concept-note-humanitarian-notification-support-access-and-protection).

Guidance and resources

Davis et al. (2020) 'Module 14, Contracting private security providers' in *Security to go: a risk management toolkit for humanitarian aid agencies,* 4th edition. GISF (https://gisf.ngo/resource/contracting-private-security-providers/).

24 To learn more, see GISF and Humanitarian Outcomes (2024).

GISF (2022) *NGO security collaboration guide* (https://gisf.ngo/long-read/ngo-security-collaboration-guide/).

GISF (n.d.a) *1. NGO security collaboration.* NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/1-ngo-security-collaboration/).

GISF (n.d.b) 'Saving Lives Together'(https://gisf.ngo/themes/coordination-for-hsrm/saving-lives-together/).

IASC (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys).

International Code of Conduct Association (2021) 'The international code of conduct for private security service providers' (https://icoca.ch/the-code/).

United Nations High Commissioner for Refugees (UNHCR) (2020) *Emergency handbook: Civil- military coordination* (https://emergency.unhcr.org/coordination-and-communication/working-others/civil-military-coordination).

UN-CMCoord (2018) UN-CMCoord field handbook. Version 2.0 (https://gisf.ngo/wp-content/uploads/2021/11/E-Version-UNCMCoord-Field-Handbook-2.0-2018.pdf).

UN OCHA (n.d.) 'Civil–military coordination' (www.unocha.org/es/node/62).

2.2 Advocacy and security

The relationship between advocacy and security in the humanitarian sector can be complex, with advocacy posing both risks and opportunities for aid worker security. Security staff can play a crucial role in ensuring advocacy efforts do not compromise security risk management efforts, but rather enhance security measures.

2.2.1 Advocacy in the aid sector

Humanitarian advocacy aims to influence the policies and behaviour of powerful actors for the benefit of crisis-affected people. This includes raising awareness of humanitarian needs, calling for the protection of civilians in conflict, and pushing for secure and unimpeded access for humanitarian activities. Advocacy frequently overlaps with access efforts and is similarly underpinned by international humanitarian and human rights law. Aid organisations may also advocate to promote specific social, economic or political changes aimed at improving the lives of marginalised or disadvantaged people.

Organisations can conduct advocacy through a variety of different means, both in public and behind the scenes.

- **Public advocacy** involves openly speaking out on issues, often through media campaigns and public statements. It aims to raise awareness, mobilise support and apply pressure on decision-makers by bringing attention to injustices or humanitarian needs.
- **Private advocacy** can involve behind-the-scenes negotiations, direct appeals and confidential discussions with government officials, armed groups and other power- or influence-holders. The goal can be to secure safe access for aid workers, influence policies discreetly or resolve specific issues without attracting public attention.

Organisations often need to balance these approaches, choosing the most appropriate method depending on the context, potential risks and desired outcomes. Irrespective of an organisation's structure and approach, however, the effectiveness of advocacy can depend on how well these align with overall

strategic goals and how they are supported by security risk management measures to mitigate potential negative impacts.[25]

There is a tension within some multi-mandate organisations between traditional humanitarian activities and advocacy work. While humanitarian work is susceptible to threats such as criminality, advocacy work presents different types of risks, such as harassment from the authorities, imprisonment, expulsion from the country, the closure of activities or the seizure of documents and computers.

In many contexts governments are adopting more extreme positions, making NGOs with political agendas prime targets, and even targeting organisations whose mandate is more focused on service delivery as opposed to advocacy. Implementing effective mitigation measures in these cases can be challenging, as aid organisations face the full weight of the governmental apparatus against them. Establishing contacts within the government and employing specialised legal experts can help to reduce these risks. While both national and international aid actors are affected, staff of national organisations are likely to be more vulnerable.

2.2.2 Advocacy and security

Advocacy can have both positive and negative impacts on the security of aid workers and the overall security environment in which they operate.

Potential negative interactions

- **Increased risks.** Advocacy, particularly when it involves challenging powerful actors or government policies, can provoke a backlash including harassment, arrests, expulsions and even violent attacks against aid workers. In countries with shrinking civic space, such as Nicaragua and Myanmar, advocacy efforts have led to government crackdowns, including the expulsion of organisations and the targeting of their staff.
- **Compromised access.** Public advocacy campaigns can lead to restrictions on access to affected populations when governments or non-state actors perceive these efforts as hostile or as undermining their authority.
- **Potential for targeting.** Speaking out on sensitive issues, such as human rights abuses, can make aid organisations and their staff targets for violence, where advocacy efforts lead to direct attacks on aid workers.

25 Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

Case example: Restricting civic space

In 2022 the Nicaraguan government enacted laws and resolutions that have resulted in the cancellation of legal registrations for over 770 NGOs and foundations, effectively forcing them to shut down. These actions have impacted a wide array of organisations, including those focused on medical services, child protection, women's rights and climate change. Since 2018 the government has revoked the registrations of more than 950 organisations, severely restricting civic space and hindering the ability of NGOs to operate and advocate for marginalised groups.

Potential positive interactions

- **Advocacy as a protective tool.** When aligned with security risk management efforts, advocacy can help enhance the protection of aid workers by promoting respect for international humanitarian law and raising awareness about the need to protect humanitarian operations. Campaigns like #NotATarget have aimed to raise awareness to help reduce violence against aid workers.
- **Leveraging advocacy for security.** Security staff can use advocacy tools to build acceptance and support for aid operations within local communities, reducing the likelihood of attacks.
- **Justice-related advocacy.** Advocacy towards justice for aid workers can include efforts to hold perpetrators accountable for attacks, harassment and violations against humanitarian staff. Organisations benefit from establishing clear protocols for when and how to pursue justice-related advocacy, ensuring any advocacy actions are informed by a robust risk assessment process.
- **Collaborative advocacy.** Forming alliances with other organisations, legal experts and international bodies can amplify the message while sharing the associated risks.

Advocacy has significant limitations. While it has had some success in achieving policy change, such as the Security Council Resolutions on the protection of aid workers,[26] in practice it has been largely ineffective in influencing state actors engaged in armed conflict: see, for example, the conflicts in Gaza and Sudan,

26 For example, UN Security Council Resolution 2730 (2024) on protection of humanitarian personnel and United Nations and associated personnel in armed conflict (https://docs.un.org/en/S/RES/2730(2024)).

where state actors have continued to obstruct and endanger humanitarian operations despite extensive advocacy efforts.[27]

2.2.3 Engaging security staff with advocacy

Security staff can play an important role in ensuring that advocacy initiatives improve security outcomes and do not compromise aid worker security.

Supporting advocacy to enhance security

- **Using security data for advocacy.** Security staff can provide valuable data on incidents, threats and the local context to support advocacy efforts. For instance, incident data can highlight areas where aid workers are most at risk, which can then be used to advocate for better protection measures from governments and armed groups.
- **Supporting public advocacy campaigns.** Security teams can assist in shaping public advocacy campaigns by providing insights into the security implications of different messages and strategies. This ensures that campaigns are not only effective in raising awareness, but also in maintaining the security of staff.

Ensuring advocacy efforts do not undermine security

- **Internal guidelines.** A structured approach with clear guidelines that integrate security considerations into advocacy efforts is beneficial. This might include protocols for speaking out, determining when and how to engage with the media and ensuring that any public statements are carefully vetted to avoid endangering staff. A good organisational policy could be to first assess the likely impact on staff and operations and seek input from security staff and staff members most likely to be affected before making any public statement about a particular situation.
- **Balanced approach.** Maintaining a balance between public and private advocacy can help ensure that efforts do not inadvertently place staff at further risk or hinder ongoing humanitarian activities.
- **Risk assessment and coordination.** Before starting any advocacy initiatives, it can be beneficial to carry out a risk assessment to evaluate the potential risks to staff and operations due to advocacy activities. This can involve analysing the political environment, understanding the potential for backlash and assessing how advocacy messages might be perceived by different actors.

27 Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

The risk assessment should ideally include consideration of the short- and long-term impacts on national aid workers and partner organisations, where applicable.

- **Mitigation measures.** Security staff can help design and implement mitigation measures to protect staff during advocacy campaigns.
- **Risk–benefit analysis.** Organisations often struggle to balance the immediate risks of advocacy with potential long-term benefits due to the lack of measurable evidence and frameworks for assessing risks. To address this, organisations could implement a risk–benefit analysis framework that compares the potential negative outcomes with anticipated positive impacts of advocacy activities. This framework could involve identifying and categorising potential risks, assessing the anticipated benefits of activities, and using a scoring system to weigh them against each other. Scenario planning can help explore possible outcomes, and mitigation measures can be developed to address identified risks. Continuous monitoring and reassessment would allow for adjustments based on changing circumstances, and documenting outcomes can help build a body of evidence to inform future advocacy efforts.

Good practice checklist

- **Leverage existing tools.** Use and disseminate established advocacy risk assessment tools, such as Oxfam's Civic Space Monitoring Tool.
- **Promote collective advocacy.** Encourage different actors (NGO forums, OCHA, donor governments) to advocate collectively, using non-operational actors for more forceful dialogue with the authorities.
- **Integrate security in advocacy planning.** Incorporate security risk management into advocacy efforts, ensuring all activities are informed by comprehensive risk assessments and implemented with risk mitigation measures in place.
- **Private advocacy first.** Share advocacy messages privately with targeted actors before going public.

- **Engage senior leadership and external messengers.** Use senior leadership, staff outside of the country or third-party organisations to deliver sensitive advocacy messages (information of abuses could be discreetly shared with human rights organisations, for example).
- **Identify escalation pathways.** Establish clear pathways for escalating advocacy messages, keeping other organisations and relevant stakeholders informed.
- **Contingency planning for pushback.** Prepare for potential pushback, including harassment or violence, by having established contacts and legal support ready.
- **Monitor advocacy impact.** Implement mechanisms to monitor both the positive and negative impacts of advocacy efforts, including on aid worker security.
- **Track and use incident data.** Track incidents of violence or harassment and use this data to advocate for aid worker protection.
- **Evaluate advocacy strategies for the protection of aid workers.** Develop tools to systematically assess the pros and cons of different advocacy approaches when addressing violence against aid workers.

Source: Humanitarian Outcomes (2024) *Aid Worker Security Report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

2.2.4 Security implications of dealing with the media

Dealing with the media

Aid organisations reach out to the media for a variety of reasons, including advocacy, which can have security implications. A poorly worded, inaccurate or inflammatory statement can put staff in direct danger and may even result in expulsion from a country. At times, a media department based in the head office and staff based in project sites can have conflicting goals. What raises an organisation's profile internationally may not help build trust with communities and local authorities. A clear system can be put in place to avoid negative incidents.

- **Media contact.** Clearly define who is responsible for media contact, drafting press releases and making public statements (including on social media).
- **Approval of public statements.** For security reasons, it is advisable for the head of the organisation in the country to have final authority over media messages, involving security, regional and head office staff as appropriate.
- **Authorised spokespeople.** Identify and train staff authorised to conduct interviews, ensuring they are well prepared. This might be limited to the senior leadership in the country or similarly qualified individuals.
- **Media strategy planning for crises.** An approach can be designed and agreed on before crises occur, with prepared statements ready for various scenarios. Engagement needs to be timely and relevant, focusing on current events to maximise impact and avoid delays.

▶ *For more on communications during crises or critical incidents, see Chapter 6.1.*

Defining goals and shaping the message

Whatever the goal of media work is – for example, to advance advocacy goals or public visibility for fundraising – organisations will want to carefully balance this against security concerns. For example, a press release blaming a particular armed group for violence against civilians could anger that group and put staff at risk. It can be helpful to prepare a list of possible questions and answers before an interview with a view to keeping messages focused, being mindful of how answers could be received in light of the context and security environment.

Setting ground rules

Media interviews require practice and expertise. It is easy to get thrown by a provocative question and say something unplanned.

- **Be careful about attributing blame for a crisis.** In many complex political emergencies, it may not be possible to say unequivocally who is responsible. It is important to agree in advance on an institutional response for the media. Staff must be careful when relaying information and make sure it has been verified by a reliable source; if it has not, they should say so clearly. Spreading inaccurate rumours could inflame tensions.

- **Ensure there is mutual understanding about 'off the record' comments.** Staff should aim to be clear with journalists when making off-the-record comments and check how the various elements of their interview will be attributed. Some common forms of light disguise in media reports, such as 'a senior UN source' or 'aid agencies operating in the conflict zone', may not be very effective. There may be only a few such aid organisations, and it might be obvious who the source was.

Finally, as mentioned previously, not all issues require media attention, and it might be appropriate to discuss possible concerns with the target actors in advance to see whether problems might be resolved through other means.

Further information

Research and discussion

Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

Legal Action Worldwide (2024) *Justice and accountability for attacks on aid workers: What are the barriers and how to overcome them?* (https://legalactionworldwide.org/accountability-rule-of-law/report-justice-and-accountability-for-attacks-on-aid-workers-what-are-the-barriers-and-how-to-overcome-them/).

Magone, C., Neuman, M. and Weissman, F. (2012) *Humanitarian negotiations revealed: the MSF experience*. Centre de Réflexion sur l'Action et les Savoirs Humanitaires (CRASH) (https://msf-crash.org/en/war-and-humanitarianism/humanitarian-negotiations-revealed-msf-experience).

Rubenstein, L. and Fairbanks, A. (2018) Evidence based advocacy: how incident information can help. GISF (www.gisf.ngo/evidence-based-advocacy-how-incident-information-can-help/).

Slim. H. (2022) *Humanitarian resistance: its ethical and operational importance*. Network Paper 87. Humanitarian Practice Network (https://odihpn.org/publication/humanitarian-resistance-its-ethical-and-operational-importance/).

Guidance

CARE International (2014) *The CARE International advocacy handbook* (https://careclimatechange.org/wp-content/uploads/2019/09/Care-International-Advocacy-Handbook.pdf).

Davidson, S. (2013) *Managing the message: communication and media management in a security crisis.* EISF (https://gisfprod.wpengine.com/resource/managing-the-message/).

GISF (2021) *Partnerships and security risk management: a joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

ICVA – International Council of Voluntary Agencies (2017) *NGO fora advocacy guide: delivering joint advocacy* (www.icvanetwork.org/resource/ngo-fora-advocay-guide-delivering-joint-advocay/).

Tactical Tech (n.d.) *Holistic security manual* (https://holistic-security.tacticaltech.org/).

Tools

Oxfam (2019) *Civic space monitoring tool* (https://policy-practice.oxfam.org/resources/civic-space-monitoring-tool-understanding-what-is-happening-in-civic-space-at-a-620874/).

Working Group on Protection of Humanitarian Action (2018) *Toolkit: responding to violence against humanitarian action on the policy level* (www.actioncontrelafaim.org/wp-content/uploads/2018/08/Responding-to-Violence.pdf).

3 Organisational elements: structures and policy instruments

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 1.2*). 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).

- 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.

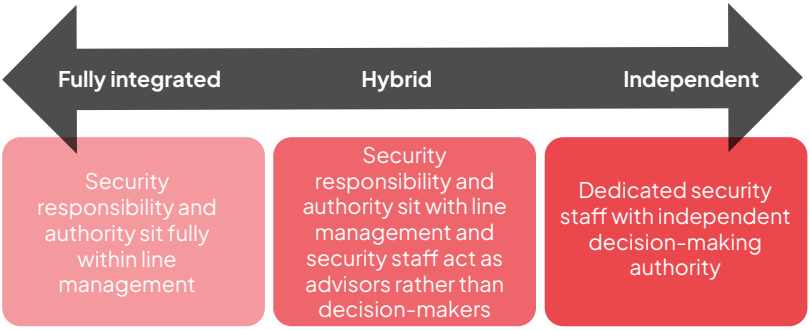
Types of security governance structures

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).

3.2 Access and security

Humanitarian access, while not an end in itself, is a prerequisite for humanitarian action. Insecurity is often a barrier to humanitarian access and, equally, efforts to improve and expand access have significant security implications.

This section defines the concept and the multiple challenges of humanitarian access as it relates to security risk management, both in the external efforts of organisations to gain, maintain and expand access and as an internal staff function. Well-established, negotiated access is essential for maintaining security in highly contested settings, both for the staff of humanitarian organisations and the people they serve.

3.2.1 Key concepts

Humanitarian access is defined as 'Access by humanitarian actors to people in need of assistance and protection and access by those in need to the goods and services essential for their survival and health, in a manner consistent with core humanitarian principles'.[33]

Access rests on two fundamental pillars: humanitarian principles and international humanitarian law (IHL), as enshrined in the Geneva Conventions and their Additional Protocols.[34] The principle of humanity obliges humanitarian actors to strive to assist all people in crisis, prioritising those most in need, while IHL stipulates that impartial humanitarian actors and operations should be protected and allowed unimpeded access by conflict parties.[35] Organisations have several tools to achieve principled humanitarian access, including high-level diplomacy, civil–military coordination and access negotiations.

Both security risk management and maximising access are essential for humanitarian action – but they are often treated as two distinct and mutually exclusive objectives. Many practitioners feel the need to strike a 'balance' between security and access in high-risk, dynamic contexts, where overly conservative management of risk can hinder the active pursuit of access to

33 UN OCHA (2012) *OCHA on message: humanitarian principles* (https://reliefweb.int/report/world/ocha-message-humanitarian-principles-enar).

34 ICRC (2014) *The Geneva Conventions of 1949 and their Additional Protocols* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

35 ICRC (2014) 'ICRC Q&A and lexicon on humanitarian access' *International Review of the Red Cross* 96(893) (https://international-review.icrc.org/articles/icrc-qa-and-lexicon-humanitarian-access).

people in need. Rather than framing it as a trade-off, however, a more productive approach uses programme criticality to guide access objectives, and uses security risk management to limit the danger in pursuit of those objectives. As a first step, it is helpful for security staff to understand the barriers to access, as well as how access efforts are undertaken in practice and how security can feed into these efforts.

3.2.2 External access challenges

Obstacles to humanitarian access come in many forms, intentional and unintentional. Humanitarian organisations typically categorise them under three broad groups:

- conflict and insecurity;
- bureaucratic and administrative impediments; and
- environmental and logistical constraints.

While security risk management is most directly concerned with the first category, all three have risk dimensions, and efforts to overcome them and expand access could usefully involve security risk management personnel.

Active conflict and insecurity

In armed conflicts, insecurity-related access obstacles include:

- threats and acts of violence directed at humanitarian personnel and assets by conflict parties;
- indirect attacks (collateral violence) affecting personnel and assets; and
- collateral damage to the operational environment, including civilian infrastructure.

Insecurity for humanitarian actors may also increase in active conflict settings due to a breakdown of social order, increased crime and illicit economic activity and acts of desperation by the population.

Armed conflict can be used as an excuse for political interference to constrain access. Particularly if the government is a party to the conflict, it may use conditions of violence and insecurity as a reason to deny or restrict access for aid groups to certain areas. Governments and militaries have been known to deny travel permits to aid organisations unless they travel with military escorts

(that they often must pay for) – an arrangement that can negatively affect public perceptions and thus create more risk than it mitigates.

Conflict parties may impose blockades on specific areas, preventing humanitarian organisations from delivering aid and essential supplies to trapped civilians. Blockades can be a tactic of collective punishment or to exert pressure on opposition groups, leading to shortages of food, medicine and other basic necessities.

Bureaucratic and administrative impediments

Burdensome, lengthy and unclear bureaucratic processes such as obtaining travel and project permits, visas or customs clearances often delay humanitarian delivery and increase operational costs. For example, in Sudan both the government and opposition forces have delayed humanitarian response by requiring multiple permissions for movements, and prevented the importation of essential medical and humanitarian equipment.

Governments can also use legal harassment and interference against humanitarian organisations, including surveillance, raids, detentions, arrests and legal challenges involving lengthy court processes. In the worst cases, organisations may be denied registration and expelled from the country. Counter-terrorism laws can restrict engagement with certain groups and impose severe penalties; excessive vetting by donors and de-risking practices by banks exacerbate these challenges. In Russia, NGOs are prevented from publicly reporting on government or military actions. Intentionally or otherwise, financial barriers, such as trade embargoes, asset freezes and bureaucratic fees, can also obstruct humanitarian operations.

Environmental and logistical constraints

Logistical and environmental barriers include lack of transport infrastructure or disruption and damage caused by climate-related events.

This type of access obstacle is not always wholly incidental or unintentional. Lack of government prioritisation of these areas and issues can be an indirect form of access denial. Selective road closures, curfews and the shutdown of services (e.g. internet and telecoms) can limit people's ability to access information and services and hinder the reach of aid organisations in areas of need. Workarounds can be costly (for example, using air assets when roads are impassable) and potentially dangerous (using alternative vehicles and hazardous routes).

3.2.3 Internal impediments to humanitarian access

Not all access constraints are external. Internal factors include the following:

- **Organisational culture and risk appetite.** Even when the desire and incentives to maximise access exist at the programming level, if the risk appetite and security risk management culture are not clear and shared at all levels, hesitation, inertia and competing priorities can limit action. For this reason, among others, it is important for organisations to integrate their strategies for improving access within their security risk management system and vice versa.
- **Systems and policies.** Organisational mandates and aspirations do not always match internal organisational procedures and processes. Discussions surrounding humanitarian access are often confined to programme and policy teams. However, support functions – such as human resources, finance, logistics, security and communication – play an equally important role in the development of access and programme strategies. Organisations that have sustainably implemented programming have effectively utilised all aspects of their organisational capacity.
- **Organisational and staff capacity.** With human resource challenges affecting the entire sector, recruiting individuals skilled in access and humanitarian negotiations can be difficult. More organisations are now turning to on-the-job training to address skill deficits.

3.2.4 Practical considerations and approaches for access

Organisations can manage access constraints with programmatic adaptations, advocacy and engagement and coordination. Access strategies often include a combination of these measures and diverse approaches to tackle the most challenging environments. For example, in Iraq during the response to the displacement crisis in 2016, organisations employed a multifaceted access strategy, which included scaling up standalone dedicated access capacity, negotiating directly with armed groups, adopting remote management programming, and participating in civil–military coordination and operational working groups.

Elements of a diversified access strategy can include the following:

- **High-level diplomacy and advocacy.** Engaging with donor governments, national authorities, international and regional organisations and other

influential actors on the protection of humanitarian workers and the responsibility to ensure unobstructed humanitarian aid. This can happen through the UN Humanitarian Coordinator or advocacy-focused NGO consortia on behalf of UN agencies and/or humanitarian organisations.

- **Interagency Access Working Groups.** Collaborating with other humanitarian organisations through umbrella mechanisms to share information and develop common strategies for improving access. This can help avoid duplication of effort while diluting risks for any single organisation. Access Working Groups are traditionally chaired by OCHA and co-chaired by an NGO. Their functions vary depending on the context, but in principle their primary objectives include information sharing, providing a safe discussion space, access monitoring and capacity-strengthening.
- **Remote arrangements or working through partners.** Partnering with local organisations and community-based groups that have established networks and trust within affected communities can facilitate access.
- **Humanitarian negotiations.** Engaging in discussions with various actors, including conflict parties, to obtain secure access to affected populations. This can range from informal discussions with checkpoint guards to formal interagency or diplomatic efforts, and involves training staff in negotiation, de-escalation and conflict mediation. Frameworks for humanitarian negotiations, such as the one developed by CCHN,[36] can provide useful tools and methods for analysing negotiation environments, assessing the parties' positions and interests, building networks, defining objectives and red lines and implementing agreements. Security staff, being across much of this analysis, may be well placed to either lead these negotiations or provide information and support. These negotiations can be conducted by individual organisations or through collective efforts (at local, national or international levels).
- **Acceptance, community engagement and outreach.** Engaging with local communities and the private sector in planning and decision-making processes to better identify local needs and barriers to access, as well as potential solutions. Adopting community-based approaches to access and security that involve regular and intentional engagement with a range of gatekeepers, including local leaders, elders and community-based organisations, can help mitigate security risks and promote acceptance of humanitarian assistance. This can strengthen and widen an organisation's network and act as an early-warning system alerting organisations to changes in the context.

36 CCHN (2019) *The CCHN field manual on frontline humanitarian negotiation*. Frontline Negotiations (https://frontline-negotiations.org/home/resources/field-manual/).

- **Information management.** Collecting and analysing data on access constraints and security risks to adapt strategies and make informed decisions. To paint a complete picture of the access environment and develop appropriate strategies, organisations can incorporate security information into broader analysis (such as political economy and conflict analysis) to understand the root causes of access challenges.
- **Supporting secure access across organisational functions.**
  - Administration: Ensuring compliance with legal and regulatory frameworks to avoid or reduce legal or bureaucratic issues that could hinder access.
  - Logistics: Developing and implementing back-up plans for the delivery of aid, including alternative transport routes and methods.
  - Security risk management: Understanding the local context and potential access constraints. Training staff to make informed security decisions and having contingency plans in place for changing conditions.
- **Technology.** Utilising technology to improve access, such as satellite imagery for context analysis, mobile apps for real-time reporting and digital platforms for remote monitoring and coordination.
- **Civil–military engagement.** Civil–military coordination for humanitarian access is rooted in IHL and guidelines developed by IASC and OCHA's Civil–Military Coordination Service.

▶ *For more, see Chapter 2.1 on security collaboration and networks.*

3.2.5 Integrating security with access to achieve programming goals

Access functions can span multiple standard positions including logistics, advocacy, programme and security teams. To address this multidisciplinary challenge, organisations have employed three different models.

- **Standalone access capacities**. Few organisations have invested in hiring dedicated staff for gaining and enhancing access. While having a standalone access position can signify the importance of access as a programme enabler, this model can quickly become expensive, harder to replicate and redundant if senior management is inexperienced in capitalising on the strengths of both security and access functions. In this model, it is important for security and access staff to collaborate as much as possible; for example, including access considerations at the design and inception stage allows for the identification of risks and the implementation of programmatic and operational adaptations, including security risk management.

- **Integrating access functions into various positions, including safety and security teams.** Some organisations have adopted an integrated security and access management approach by combining the positions. While this model is less resource-intensive and could avoid confusion between roles and responsibilities, its success is likely dependent on the organisation's ability to develop a job description that adequately includes both functions and subsequently recruit the right profile. This can be especially difficult if security specialists are recruited from the police or the military.

Case example: The Safer Access Framework – an integrated model

The Safer Access Framework (SAF), developed by the ICRC to support Red Cross and Red Crescent national societies in gaining safe access to affected populations, has eight categories of measures to enhance acceptance, security and access. These include understanding the local context and risks, situating the organisation within legal and policy frameworks, building and maintaining acceptance among local stakeholders, ensuring the organisation's visibility, ensuring effective internal and external communication and implementing a robust operational security risk management system.

This approach recognises the links between acceptance, security and access, and provides key measures for enhancing all three. In practice this has meant, for example, ensuring security and acceptance-building practices are incorporated into volunteer training, strengthening communications teams to monitor public perceptions and safeguard the organisation's reputation online, and establishing local office coordination teams that work across different departments and programmes to implement SAF principles and priorities.

For further information, see https://saferaccess.icrc.org

- **Hybrid model.** Some organisations have split operational access responsibility and technical support. At the head-office level, technical access experts sit separately from security teams and provide guidance and advisory functions to country teams, including training and strategy development. At the regional and country level, day-to-day operational access is managed by security teams. This model provides in-house technical access capacity while acknowledging the difficulty of hiring additional dedicated staff at the country level. However, it does not address the issue that the technical teams do not have a technical line to security staff at the regional or country level, meaning that quality control is dependent on whether the right profiles have been recruited across security functions, and the strength of the relationship between the access team and individual country directors.

Further information

Research and discussion

ACAPS (July 2024) 'Humanitarian access' (www.acaps.org/en/thematics/all-topics/humanitarian-access).

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

Magone, C., Neuman, M. and Weissman, F. (2012) *Humanitarian negotiations revealed: the MSF experience*. Centre de Réflexion sur l'Action et les Savoirs Humanitaires (CRASH) (https://msf-crash.org/en/war-and-humanitarianism/humanitarian-negotiations-revealed-msf-experience).

UN OCHA (2012) 'OCHA on message: humanitarian principles' (https://reliefweb.int/report/world/ocha-message-humanitarian-principles-enar).

Guidance and resources

CCHN (2019) *The CCHN field manual on frontline humanitarian negotiation*. Frontline Negotiations (https://frontline-negotiations.org/home/resources/field-manual/).

ICRC (n.d.) *The Geneva Conventions of 1949 and their Additional Protocols* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

ICRC (2015) 'ICRC Q&A and lexicon on humanitarian access' *International Review of the Red Cross* 96(893) (https://international-review.icrc.org/articles/icrc-qa-and-lexicon-humanitarian-access).

ICRC (n.d.) Safer access for all national societies. Overview (https://saferaccess.icrc.org/overview/).

3.3 Funding security risk management

No matter what mix of security risk management measures aid organisations employ, they will inevitably entail costs. These costs, like the measures themselves, must be considered from the earliest stages of programme design and built into proposal budgets. Ensuring that adequate funding is available to enable organisations to operate securely is vital, and a subject on which organisations and their donors should be prepared to have frank discussions. This chapter shares good practice around budgeting for security-related expenses and highlights some of the key issues and developments in donor funding and coordination initiatives.

3.3.1 Costs and budgeting

There are no uniform budgeting formulae or common expenditure definitions for inputs and activities designed to enhance operational security. Organisations and donors vary in how they budget for security-related costs. Some include security funding in overhead costs or support services, others include it as a separate line item or as a fixed percentage of programme costs, or fully integrate security costs within their programme costs. For example: vehicles needed for staff to travel in convoys would go into the 'vehicles/transport' line; installing physical security measures like gates or alarms would come under 'facilities repairs/maintenance'; and security risk management professionals might fall under 'support staff'. Similarly, staff members with skills in negotiation or community liaison are often vital to implementing acceptance measures for security risk management, but may not be labelled as security-related costs.

It is now generally recognised that effective security risk management is essential for sustainable programme implementation so should ideally not be considered an overhead cost. When donors instead require estimates for security costs in proposals (as some major donor governments do), it not only allows organisations to include the necessary inputs but also prompts them to actively think through security needs as part of the budgeting and programme design process. Like many other facets of security risk management, security costing and budgeting derive primarily from the risk assessment, which can guide the allocation of attention and resources. The risk assessment can also include consideration of the risks faced by partner organisations working on the programme, and these costs incorporated into any proposal. In sum,

security risk management costs can refer to any expense related to reducing the potential harm or loss to the organisation, its staff and partners, or responding to and compensating for actual harm or loss, while maximising the potential for successful operations.

To meet its duty of care, an organisation's security risk management measures must be commensurate with the amount of risk its staff face while carrying out their work. Not budgeting appropriately for foreseeable risks would be negligent. This requires open and direct communication with donors and relevant organisational teams not just at proposal stage but throughout the programme lifecycle, as security conditions may evolve. It also requires that organisations understand and document the costs incurred for managing security risks, which can then demonstrate value for money to donors in that they enabled aid programming to proceed.

Budgeting for security at the project/programme level must usually follow donor requirements, but organisations will often also need a general policy on security budgeting that is organisation-wide and not dependent on individual project budgets that have end dates. Using core funding, whether obtained through cumulative overheads, unrestricted funding or specific grants, can allow for sustainable security risk management functions, structures and staff positions that cut across projects and years. This can be difficult to achieve for local organisations, which have far more limited access to core funding than international organisations, so are at a structural disadvantage when it comes to strengthening their organisational capacities.

Budgeting for security

GISF's Risk Management Expense Portfolio (RMEP) is a spreadsheet budgeting tool offering guidance on the full scope of tangible and intangible security costs in areas such as assets and equipment, salaries and training. The tool presents the following budget categories, which security expenses may fall under as direct costs:[i]

- salaries
- admin and logistics
- training, learning and development

- information and knowledge management
- access
- facilities management
- communications assets
- medical assets
- transport assets
- crisis management assets
- insurance
- general contingency funds (e.g. for critical incident response or evacuation).

An additional note: including explanatory notes within the budget for each line item, cross-referenced with the text in the proposal narrative, can be a powerful tool in justifying costs.

[i] For further details, see www.gisf.ngo/resource/the-cost-of-srm-for-ngos/

3.3.2 Internal processes

A challenge arises when staff responsible for developing proposals and budgets do not have oversight of security risk management needs or do not adequately engage those that do. This raises the risk that security-related costs are not adequately budgeted for, or that, in the event of budget cuts, these costs are the first to be removed.

It is a mistake to design an aid programme and determine how to 'make it secure' after the fact. To truly enable humanitarian action, security risk management must be integrated into programming at all stages. This requires close collaboration between programming, finance and grant management, security risk management, logistics and other relevant staff from the initial stages of design and proposal development, as well as at any change points, such as budget modifications or no-cost extensions. It is advisable for organisations that have dedicated security risk management advisors or managers to ensure that these staff members are involved from the outset, working collaboratively rather than

in isolation. Additionally, they can develop skills in budgeting processes in order to engage effectively with finance and grant management colleagues.

Staff of organisational partners within a programme or project should ideally also be involved in key planning and budgeting meetings, to ensure that the security risk management needs of all partners are considered in the budgeting process from the earliest stages.

▶ *See more on security funding between partners in Chapter 3.5 – Security risk management in partnerships.*

Case example: Budgeting for security

One international organisation's security staff begin planning for programme security risk management costs during the operating budget development phase for the coming fiscal year. This ensures that overarching and non-project-specific security-related costs are accounted for in the shared programme costs for the fiscal year, and reduces the time it takes to outline and include these costs in any specific project proposal. These costs could include learning and development, supplies and equipment and admin and logistics. Project-related cost proposals aim to accurately reflect the added costs of maintaining the organisation's safety and security policy and standards.

The organisation also ensures that its budget development phase involves coordination with relevant colleagues from human resources, admin, finance, supply chain, partnership and others to ensure there is no duplication or elimination of costs for items that may be related to safety and security, but are managed by those departments.

3.3.3 Donor engagement

Generally speaking, the major governmental humanitarian donors are prepared to fund appropriate and justified safety- and security-related expenditures. Explicit references to security risk management and related expenditures are contained in the proposal guidelines of a few official donor agencies and a small number of donors have specific security risk management and coordination units or focal points, which can provide useful guidance, particularly during programme planning and the initial budgeting stages. Some donor agencies have also organised meetings and workshops to advise aid organisations on how to include security costs in proposals. While some donors do not actively ask for security risk management costs to be included in a proposal, they may fund these costs if they are presented and justified.

When international organisations subgrant or subcontract to local organisations, however, they may not offer or allow for security risk management costs in the budget. This can create a moral hazard, where the local organisation is incentivised to take risks and refrain from including security inputs in its budget to be more competitive in the quest for international contracts. While being mindful of not creating additional unnecessary bureaucracy, international organisations can aim to ensure the same level of open discussion, clear communication of needs and on-paper planning around security risk management with their implementing partners as with their donors. Ideally, partnerships will include a component of core costs to allow the local organisation to develop sustainable security risk management capabilities.

While donors vary in what they will fund, common areas of expenditure include communications equipment, physical security items and upgrades, security training, safety equipment, first aid/emergency kits and security personnel (either partially or fully, depending on the risk level of the context and the donor). Additional operational-level security support, such as that offered by private security providers, is normally considered on a case-by-case basis.

Some donor government agencies actively encourage greater security awareness and security competencies within the aid organisations they fund, and expect to see security-related expenditures in budgets. Proposals may have to be accompanied by a detailed security plan that includes a context analysis and risk assessment. In order to avoid significant revisions to project budgets once contracts have been signed, risk assessments may describe possible future scenarios – and future needs – should security deteriorate. Beyond this,

however, donors tend not to dictate particular security policies or practices, preferring to leave organisations to determine their own security stance and exercise their own quality control over this area. In part, this is because donors lack the staff time, competence and operational presence to exert more direct influence. Donors are also wary of being seen to impose a particular security model on organisations. Getting formally involved in quality assurance would also potentially expose donors to liability claims. Many donors do not explicitly ask for security budgets, and security professionals have come across some that state they will not fund security. In cases where there is no explicit security budget line, security-related costs can be covered through other budget lines.

Donor involvement beyond funding operational security needs

While donors will never take on responsibility for an organisation's security risk management, several have provided additional resources to strengthen aid organisations' own security risk management efforts. For example, government donors supported interagency capacities and competencies by providing funding for GISF and INSO. Government donors have also funded research to examine evolving challenges in security risk management and to assess current security practice among aid organisations.

Donors also contribute funds to UNDSS for additional staff and activities, with a particular focus on NGO liaison responsibilities through the Saving Lives Together initiative and sector-wide security supplementation, for example for additional training on personal security and first aid.

As organisations often fund programmes with contributions from multiple donors, coordination between donors is important (but currently limited) to ensure coherence in security budgeting requirements and guidelines.

Some donors require visibility for their funding and maintain branding policies that require their logos to be displayed on the assets they pay for, including offices, vehicles and relief items. In some cases, this association may be deemed a security threat, particularly if the donor in question is unpopular in the particular context, or if the organisation is trying to adopt a low-visibility approach. In such cases, an organisation may formally request a waiver of the visibility requirement. Donors can be flexible about these requirements when security concerns dictate caution.

Further information

Research and guidance

EISF (2013) *The Cost of Security Risk Management for NGOs* (www.gisf.ngo/resource/the-cost-of-srm-for-ngos/).

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).

Stoddard, A. and Harmer. A. (2010) *Supporting security for humanitarian action: a review of critical issues for the humanitarian community.* Humanitarian Outcomes (www.humanitarianoutcomes.org/publications/supporting-security-humanitarian-action).

Government donor funding policies and examples

Civil Protection and Humanitarian Aid Operations (ECHO) (2023) 'Humanitarian implementation plans (HIPs)'. Thematic policy annex 2024. General considerations: safe and secure provision of aid (https://ec.europa.eu/echo/files/funding/hip2024/thematic_policies_annex_2024.pdf).

Foreign, Commonwealth & Development Office (FCDO) (n.d.) *FCDO humanitarian funding guidelines for NGOs applying for CHASE humanitarian response funding.* Annex B: Budget template (www.gov.uk/guidance/humanitarian-response-funding).

3.4 Monitoring for compliance, effectiveness and impact

A critical component of security risk management is ensuring that policies, plans and procedures are regularly reviewed and evaluated to measure compliance, effectiveness and impact at an organisation-wide and location-specific level.

3.4.1 Monitoring mechanisms

Monitoring security risk management compliance, effectiveness and impact can ensure that security enables the organisation to achieve its objectives and supports its programmes effectively. Monitoring is an important element in meeting duty of care obligations and can provide essential information to identify strengths and weaknesses, allowing organisations to focus resources where they are most needed.

A key challenge with monitoring mechanisms, however, is when they are perceived as impediments to programme implementation, creating additional burdens and layers of bureaucracy. An additional concern is where the approach is compliance-led, i.e. focused primarily on making sure minimum requirements are met, rather than looking at the effectiveness of the measures in place. To address this, monitoring mechanisms have to be adaptable and scalable. They should aim not to overwhelm managers or be used to construct a security set-up that is not needed (even if this is well intentioned) and that can become an impediment to fluid programming. It is advisable to have different monitoring measures for low- and high-risk environments, and commensurate with – and adapted to – needs and capacity. Monitoring mechanisms can also offer security teams the opportunity to take a step back and ask why an organisation is using the tools and processes that it is and whether things could be simplified, and to ensure that security is supporting all staff in meeting organisational and programmatic objectives.

Effective monitoring supports organisational learning. This can be particularly challenging when there is a lot of information to absorb, and it is especially important that knowledge and learning are not confined just to the security teams. At the most basic level, the findings and recommendations of security audits and other relevant monitoring mechanisms should be communicated to those who participated and, where possible, be accessible to wider staff.

Sharing the outcomes of these processes can support transparency and raise awareness of how security staff are taking forward information gathered to create a more secure and enabling work environment.

Monitoring efforts can be grouped into three interrelated (and sometimes overlapping) areas.

- **Compliance.** Regular review of the implementation of security risk management practices, including regular reporting and monitoring of key indicators to ensure things are working and whether changes are needed. Dashboards play a helpful role in this.
- **Effectiveness.** Periodic deep dives into processes to measure the effectiveness of security practices and systems, including formal security audits.
- **Impact**. In-depth analysis using information from monitoring efforts and other sources to understand whether the organisation's security risk management system is influencing or contributing to change.

These are discussed in more detail below.

3.4.2 Compliance monitoring

For compliance monitoring, organisations can use a combination of methods, such as checklists and key performance indicators. The purpose of compliance monitoring is primarily to understand the reasons behind non-compliance, not to penalise staff. It may be that processes are not being followed because they are unrealistic or unsuitable for the context. Non-compliance can also reveal challenges, such as insufficient resources, negative perceptions of security practices among staff and knowledge gaps. Monitoring of this nature can help identify gaps and challenges that need to be addressed, including training, guidance, support or other positive security culture-building activities. Some examples of compliance monitoring measures are in Table 2.

Table 2 Example compliance-monitoring measures

Measure	Information
Checklists	A checklist helps in assessing compliance with security policies and minimum requirements, particularly at office or project level. A checklist can help managers quickly verify that the information they are receiving from staff is correct.
Key performance indicators (KPIs)	KPIs measure and track performance against strategic and operational goals. They are used for decision-making and performance improvement. KPIs can serve multiple functions in monitoring compliance. They can be linked to individual roles and responsibilities, particularly those of managers and staff, who are accountable for security compliance. Programmes and offices can also have security-related KPIs, such as percentages and numbers relating to, for example, updated security plans, security briefings for travelling staff, number of trained staff, percentage of security funding in the overall budget, forecasted versus actual budget granted and consumption of security funding and coverage of needs. Some security KPIs may also be global. Dashboards can be particularly helpful in monitoring KPIs, particularly in tracking indicators across different offices, countries and regions (see the section below for more details on dashboards).
Staff appraisals	Senior staff members and others accountable for security risk management may be appraised to evaluate their performance in security-related areas of work. In most cases, all staff, regardless of their position, will be expected to comply with security rules, and share relevant information with security staff. Team leaders can also be appraised in relation to how they and their teams have complied with the security risk management system. To support this, security elements will need to be included in recruitment processes, such as job descriptions and interview questions.

Measure	Information
Regular security reporting	Regular quantitative and qualitative security reporting and analysis can provide an overview of security risk management practices and their implementation. Regular reports can help accountable staff understand if minimum requirements are being met, identify challenges and gaps and prompt corrective measures. Regular reporting and monitoring can reduce the likelihood of unexpected outcomes and findings from more formal audits. Indicators for regular reporting could include: • Validity/expiry of security plans. • Changes in security levels. • Number and severity of incidents and people affected. • Budget available for security and the amount spent. • Number of staff trained in security versus organisational targets. Online tools can support the monitoring of some key indicators. For example, organisations that have online training resources can quickly provide compliance information, when needed, about training up-take.
Incident reporting and analysis	Monitoring the number of incidents affecting a particular location can provide an overview of trends and signal when security risk management processes may need more attention. However, this can be misleading without a reference value or baseline, as increases might indicate improved reporting rather than heightened insecurity. Besides incident numbers, monitoring how reports are managed – such as delays in submission, the completeness of reporting templates and levels of under-reporting – can help assess compliance with security practices. Incident analysis also supports affected individuals and serves as an alert for evaluating the effectiveness of risk assessments, mitigation measures and the overall security risk management system. It also helps identify compliance issues or gaps in procedures, support and training by analysing the type, frequency and causes of incidents involving staff. (*See Chapter 4.4 for more on incident reporting.*)
Post-incident/ crisis reviews	Similar to incident analysis, an in-depth evaluation following a critical incident or crisis can provide an overview of compliance with security measures, and their relevance and effectiveness.

Senior managers should provide feedback to encourage reporting and implementation of other compliance mechanisms. The findings of this monitoring, including reports, can be made available to managers and other relevant staff and shared by email, in meetings or via a dashboard (see below).

Improving security risk management through monitoring may sometimes mean holding staff accountable for a failure to comply with policy and procedures. In the event that evidence of non-compliance merits penalisation, it is important that organisational policy regarding this is adhered to transparently. Organisational policy in this regard should be well communicated to staff beforehand. The aim should be to support a positive security culture, rather than create further disincentives or animosity towards security processes.

Case example: Building relationships to improve compliance

One international NGO found that compliance and overall security culture improved following an overhaul of how the security team engaged with other staff. This involved removing security jargon from communications and taking other measures to build trust and make the security team appear more approachable. Efforts were made to recruit security staff from diverse backgrounds and to encourage staff to see the security team as an essential and helpful resource. Outreach activities were also put in place, including monthly security sessions and meetings with different organisational teams. A shift in tone by organisational leadership on the role of security as an enabler for staff to carry out their work was also fundamental to this shift.

Security staff also benefit from being creative about how to promote compliance, including looking at different kinds of incentives. Rewards, as well as naming-and-shaming measures, have been effective in some cases. For example, some international organisations use organisational forums to list country offices that are not compliant or fail to meet primary KPIs. Dashboards can be an effective tool for this, as illustrated in the section below.

3.4.3 Effectiveness monitoring

To monitor effectiveness, more organisations are now undertaking security audits, reviews and consultations. These go beyond compliance monitoring, and take a deeper look at the implementation and effectiveness of security measures and systems.

Security audits

A security audit's primary aim is to examine whether an organisation's security risk management measures are enabling it to meet programme objectives without exposing the organisation and its staff to avoidable risks. The outcome of a security audit should ideally be an action plan that supports staff in carrying out their work safely and securely (Figure 6).

What a security audit looks like, how regularly it takes place, who does it and how in-depth it is will vary from organisation to organisation. However, security audits can be broken down into two broad categories: organisation-wide, and location-specific.

Security audits, particularly location-specific ones, can be used to verify that the mitigation measures identified in the risk assessment and security plan were implemented, and assess the extent to which policies and procedures were followed. Security audits can help determine if the initial assessments and plans are still relevant, and can be used to verify that regular security information (e.g. through security reports) from a particular working location is accurate.

Audits can be ad hoc or carried out on a regular basis. Location-specific audits are carried out in accordance with organisational-level policies. Although security audits are usually announced in advance, they may not always be.

While different organisations will develop their own audit processes and tools, including key indicators, GISF (formerly EISF) Security Audits guide[37] and the Swiss Centre of Competence for International Cooperation (CINFO) Duty of Care Maturity Model[38] offer example indicators that can serve as templates for assessing how an organisation is performing in the security sphere.[39]

37 Finucane, C. (2013) *Security audits.* EISF (https://gisf.ngo/resource/security-audits/).

38 See https://dutyofcare.cinfo.ch/

39 The EISF (now GISF) *Security Risk Management: A Basic Guide for Smaller NGOs* provides a quick reference guide across a number of security-related elements that can be helpful for planning an audit or review: https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/

Organisations benefit from mapping indicators and results against security systems, frameworks or requirements.

Audits versus reviews

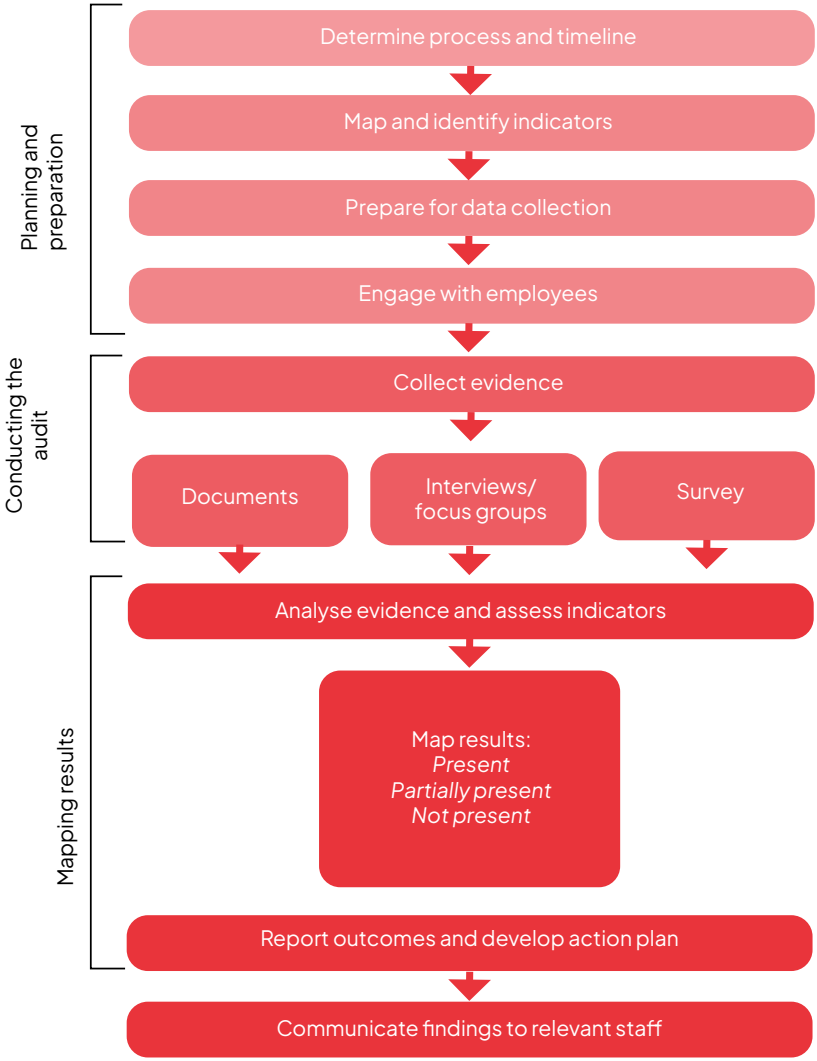
A security audit is a formal, compliance-focused assessment of an organisation's security policies, procedures and practices against established organisational requirements and indicators. In contrast, a security review is often a more flexible, informal process that assesses the effectiveness of security measures, identifies weaknesses and provides recommendations for improvement, focusing on enhancing overall security rather than just compliance. Security audits are planned, whereas reviews are more likely to be carried out after a critical incident or following a sudden change in the context.

Some organisations also carry out global or organisational reviews of security systems and approaches, which are formal evaluations based on specific terms of reference. These often go beyond an assessment of internal standards or requirements; while they might be benchmarking against common approaches and good practice in the sector, there are no specific external standards being audited against – so they are often referred to as a review and not an audit.

Some organisations have chosen not to use the term 'audit' given the negative connotations attached to it, preferring terms like 'reviews' or 'checks' to move away from the perception that the reviewers are assessing individual performance or seeking to find fault in staff members' work. Therefore, what is considered an 'audit' versus a 'review' will vary by organisation.

Both security audits and reviews assess the 'health' of security systems and staff awareness and understanding of security measures and resources. These evaluations offer staff an opportunity to highlight security risks or challenges they face in their lives and work, which might not be adequately considered by existing security measures.

Figure 6 Security audit process



Adapted from Finucane, C. (2013) *Security audits.* EISF (www.gisf.ngo/resource/security-audits/).

Audits can include a review of relevant documentation, incident data, interviews, focus group discussions with key staff and surveys. They can be time-consuming.

Security audits should ideally involve consultations with a wide pool of staff, not just those with security risk management responsibilities. Collection of relevant data and the assessment of key indicators are followed by an analysis of the findings, presentation of the results and an action plan. An action plan lists specific activities to be carried out, identifies those in charge, prioritises what should be done first, establishes a timeframe and quantifies the budget needed for implementation.

In some cases, it may be advisable for security audits to be carried out by external reviewers or consultants. This can result in more objective results and can also serve to benchmark an organisation against its peers by drawing on insight from the external reviewer. In some cases, an external reviewer may also elicit more candid responses from staff members on the effectiveness and weaknesses of the security risk management system. Where the cost of an external reviewer may be an obstacle, organisations sometimes work together to carry out peer reviews.

Case example: Audit process

One international NGO has developed an extensive safety and security audit process, which has been running for several years. Each year, several countries are audited. External auditors are brought in to carry out a mix of in-person and remote consultations. The audit is conducted against over 100 KPIs. The auditors produce a KPI report (which is compliance-focused) and a narrative report that looks at the effectiveness of the overall security system: what is working well, what the gaps are, and recommendations.

Measuring acceptance

An inherent weakness of security audits, and all monitoring mechanisms, is the tendency to focus on easily collected and analysable data, with a particular bias towards quantitative data (such as the percentage of staff trained and number of security incidents). This can lead to a focus on protective activities, which are more tangible and more easily recorded than acceptance measures.

Security monitoring mechanisms can measure acceptance and perceptions by drawing data from programmatic monitoring activities and perception surveys, developing and implementing additional tools (such as acceptance analyses) or incorporating acceptance metrics into existing tools, such as actor mapping. Programme evaluations can provide a way of monitoring perceptions and acceptance, but they seldom feed into security risk management monitoring efforts.

The Acceptance Research project and the Acceptance Toolkit provide some useful tips on how to assess acceptance: https://acceptanceresearch.wordpress.com. *See also Chapter 4.2 – Developing a security strategy.*

For tools and guidance on how to monitor acceptance more regularly see, for example, GISF's acceptance analysis template (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/) and Chapter 4 of *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Consultations

Ad hoc staff consultations on challenges and weaknesses are becoming increasingly common in the aid sector. These often follow a complaint or reports of misconduct or negligence, and can relate to issues such as racism, sexual exploitation and abuse, harassment and bullying. Security teams can use the learning from these consultations to improve their work, and may also benefit from carrying out their own consultations on particular security-related topics.

Confidential reporting and whistleblowing mechanisms can help organisations uncover poor security practices.

Case example: Consultations

An international NGO consulted over 2,000 female staff across multiple countries to understand their security concerns. The findings led to a global report and action plan and a shift towards addressing identity-based risks institutionally. Future consultations are planned for other identity-based risks and concerns.

3.4.4 Impact evaluation

Impact refers to the changes – both intended and unintended – that occur as a result of an organisation's activities. Impact measurement is the process of evaluating these changes, both qualitatively and quantitatively. It assesses how much of the observed change can be attributed to specific actions taken by an organisation.

To measure impact, organisations can apply a theory of change approach, which involves creating a detailed roadmap that outlines the desired long-term outcomes, such as creating a safer work environment, and the steps needed to achieve them. The process usually involves breaking down the long-term goal into intermediate outcomes, like improved crisis management and reduced incident rates, which can be monitored over time, and supported by specific activities, such as security training and crisis management planning. It is advisable to identify suitable indicators of positive and negative change, with a focus on determining causality (i.e. how much of the change was due to the influence or contribution of security risk management practices and systems). The monitoring mechanisms outlined in this chapter can help with evaluating impact.

The focus of impact evaluation exercises need not be on finding conclusive proof that an intervention has contributed to a change or set of changes. Instead, the process can focus on producing a plausible, evidence-based narrative that indicates impact. Evidence learning questions can be useful in this exercise (see the box below for examples).

Example evidence learning questions

- To what extent are the organisation's security training programmes improving staff awareness and behaviour regarding security risks?
  - Training attendance records, pre- and post-training assessments, staff feedback surveys and observed changes in behaviour or decision-making.
- What impact have security incidents had on the organisation's ability to deliver humanitarian assistance?
  - Records of operational disruptions, delays or changes in programme delivery due to security incidents. Interviews with staff about how security incidents have affected operations.
- Are there observable improvements in security risk management outcomes compared to previous periods and other peer organisations operating in the same areas?
  - Historical data on security incidents, trend analyses (compared with other organisations) and comparisons of risk management effectiveness over time.
- What lessons have been learned from recent security incidents, and how have they been applied to improve practice?
  - Post-incident reviews, action plans, documented lessons learned, changes made to policies or procedures based on these lessons and follow-up on the effectiveness of these changes.
- How have security measures impacted employee retention and recruitment? (A safe work environment can be a key factor in attracting and retaining staff.)
  - Turnover rates by location versus security indicators, feedback from exit interviews (reasons for leaving), the number of job applicants and their feedback on the company's security reputation.

3.4.5 Data visualisation and dashboards

Organisations increasingly use digital dashboards in security risk management. A dashboard is a collection of key metrics and data points displayed on a single platform in real time. Dashboards facilitate data visualisation in various formats, such as maps, KPIs, tables and charts. These tools can be accessed both publicly and privately, and mobile compatibility is increasingly common.[40]

Dashboards support numerous applications in security risk management, including visualising security levels and travel restrictions by location; storing and accessing risk assessments and security plans; monitoring compliance; displaying incident figures; and helping identify gaps to prioritise funding and other support. They also aid in briefing new recruits, preparing reports and tracking budget allocations. Real-time data such as this enables organisations to take corrective measures promptly, negating the need to wait for periodic reports or updates.

When designing a dashboard, it is crucial to define its purpose, the information required to support it, data collection methods, roles and responsibilities and access permissions. Various data visualisation solutions are available to purchase, with some free up to a certain usage level. Compatibility with existing systems is an essential consideration.

Case example: Dashboards, compliance and impact

A large international NGO invested in improving the rate of valid security plans, simplifying the format and doing a closer follow-up, for which a dashboard turned out to be essential. The dashboard inadvertently created a 'healthy competition' between country teams to show who was doing better in meeting security requirements. Before the introduction of the dashboard, the organisation was struggling to improve compliance. Plans were not updated before the expiration date, and there was little visibility from and among country, regional and global offices.

40 For an example of a publicly accessible dashboard, see INSO: https://ngosafety.org/conflict-data-dashboard/#dashboard

Thanks to the dashboard, managers were able to see how their countries and regions were doing in terms of compliance, using a simple traffic light colouring of data. The dashboard was then posted on the security team's intranet and shared with decision-makers.

A security KPI was created based on the number of security plans that were up to date, visible to staff in country, regional and global offices. One year after the introduction of the dashboard, the indicator increased to 70% simply by making the data visible to staff. In the second year, it had increased to 79%.

Reliable dashboards require pertinent, reliable and accessible data – both internal and external. Processes for data collection and management must be established, with safeguards for confidentiality. Dashboards should aim to balance the need for information sharing with confidentiality requirements and data protection regulations, ensuring that sensitive information is handled appropriately.

Data visualisation tools are designed to be shown and shared, and to help managers make decisions. Any tension between confidentiality and information sharing should ideally be tackled during the design and planning phase.

Further information

Guidance and research

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/).

Billaudel, R. (2021) 'Measuring and improving acceptance: ACF's experience and perspectives' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Finucane, C. (2013) *Security audits*. EISF (www.gisf.ngo/resource/security-audits/).

GISF (2024) *Security Risk Management (SRM) Strategy and Policy Development: a cross-functional guide* (https://gisf.ngo/resource/srm-strategy-and-policy-guide/).

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).

Tools

Collaborative Learning Approach to NGO Security Management (2011) *Acceptance toolkit* (https://acceptanceresearch.wordpress.com/acceptance-toolkit/).

GISF (n.d.) 'Acceptance analysis template - xlsx'. *2. Acceptance analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

INSO (n.d.) *Conflict data dashboard* (https://ngosafety.org/conflict-data-dashboard/#dashboard).

CINFO (n.d.) *Duty of care maturity model* (https://dutyofcare.cinfo.ch/model.html).

3.5 Security risk management in partnerships

In aid work, it is common for part or all of a programme to be designed and 'owned' by one organisation, but implemented in part or wholly by another. Working with and through other organisations or associations may be more cost-effective, programmatically sound or part of a deliberate strategy, such as to strengthen local capacities or reduce risk. The number of partnerships in the aid sector has increased in recent years, due in part to localisation and decolonisation efforts. This chapter examines equitable partnerships through a security lens. While it acknowledges the diversity of aid sector partnerships, and aims to be broadly applicable, it focuses on partnerships between international organisations and national and local actors.[41]

3.5.1 Principles and strategic considerations

A partnership is any formalised working relationship between two or more organisations to meet agreed objectives. Partnerships in the aid sector can vary in form, length, scope and degree of collaboration; they can be strategic and long-term, or project-based and short-term. They are often bilateral between international organisations and national actors (e.g. local NGOs and community-based groups), but can also be between several organisations (such as through consortia and umbrella grants), and between organisations and private companies, as well as between national NGOs. For some international organisations, implementing through local partners may be their core way of working, while for others it may only be an occasional departure from direct implementation by their own staff.

Partnership agreements or contracts tend to dictate the scope of these types of arrangement, with security responsibilities sometimes marked in agreements as falling under each individual legal entity. In some circumstances, agreements can dictate a cross-over of support, e.g. in the event of a critical incident. In many cases, however, responsibilities are unclear, and cooperation on security risk management is not spelled out, leading to wide variance in how these issues are handled.

41 Some literature distinguishes between 'national' and 'local' organisations and actors. This GPR uses both terms interchangeably to refer to all types of organisations that operate solely in one country, whether in multiple locations or just one, including community-based groups.

The growing calls for 'localisation' within the aid sector have, unfortunately, not resulted in a commensurate discussion of security risk management and duty of care considerations in international–local partnership arrangements. This is often to the detriment of local actors, who often face the greatest risk of experiencing a severe security incident, but receive the least security support (both within their organisations and from their international partners).[42] Research has also shown that, in international–local partnerships, the risks most discussed and mitigated against are fiduciary, while security risks are often dealt with perfunctorily. While this seems to be changing, challenges remain.[43]

Whether and how partnership arrangements consider security risk management can often be a reflection of:

- how much each partner organisation internally considers and addresses security risks; and
- the circumstances and objectives of the partnership.

Organisations that lack knowledge or capacity, or where robust internal security risk management systems are not in place, may feel unable to have security discussions or extend support beyond their own organisation and staff, or may not have the organisational security culture to even consider doing so. Engagement can also differ within the same organisation due to varying capacities in security risk management across different offices and locations.

The intentionality or purpose of a partnership also affects how the partnership is viewed and managed, with consequences for how partners discuss the risks they face in carrying out their work. For example, research into local–international partnerships has shown that short-term, project-based partnership models are not conducive to security risk management discussions or support.[44]

42 GISF (2020) *Partnerships and security risk management: from the local partner's perspective* (https://gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/); 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).

43 Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local–international partnerships (global report)* (https://humanitarianoutcomes.org/publications/ngos-risk2-partnerships); GISF and Humanitarian Outcomes (2024).

44 GISF (2020).

3.5.2 Challenges

Partners face a number of challenges and obstacles when trying to engage in mutually beneficial security risk management.

Duty of care – legal and ethical considerations

As discussed in Chapter 1.1, 'Key concepts and principles', legal duty of care is generally understood to apply solely to an organisation's own employees, rather than to those of partner organisations. Nevertheless, there exists an ethical duty to support partners in managing security risks and to share pertinent information, knowledge and good practice. Some international organisations are concerned that, by offering such support, they might inadvertently assume legal liability for the staff of their partners. Some security staff have been advised by legal counsel to refrain from engaging with partners on security matters for this reason.[45]

While the extent and nature of legal responsibility can vary significantly depending on the jurisdiction and specific circumstances, these concerns may be exaggerated. As with individuals,[46] an organisation's legal responsibility towards a partner may depend on the 'degree of control' it exerts over the partner's decision-making processes.

While it is good practice to consider the relevant legal instruments and their implications on security risk management within partnerships, ignoring the issue altogether is an ethical failing that could, potentially, lead to legal consequences. In general, it is beneficial for every organisation that enters into partnerships regularly to establish a policy on what kind of support the organisation will provide or expect from its partners. In addition to making clear where responsibility sits, the support provided to partners on security should aim to remain collaborative, without dictating one particular approach over another, and keep decision-making clearly within each organisation. In this respect, it is important to also be cognisant of how power imbalances and financial incentives can make 'support and advice' appear like direction. In some jurisdictions, a legal

45 GISF and Humanitarian Outcomes (2024).

46 An organisation's legal responsibility towards an individual can be relative to the 'degree of control' the organisation has over that individual's circumstances. For example, an organisation that is hosting a visit from a non-employee in a particular country, and that has full control over where the visitor is staying, their travel arrangements and general itinerary, will likely have a de facto legal duty of care to that individual, whether or not a contractual agreement is in place. See Kemp, E. and Merkelbach, M. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications.* EISF (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

entity may be held liable if it were to emerge that an agreement was harmful to one party, even if both agreed to it. This is a particular concern as implementing partners may feel pressured to take on more security risks than they are comfortable with in order to gain contracts. To address this, partners can prioritise building trust with each other and developing strong communication around these issues.

Risk transfer

Sometimes, international NGOs partner with local actors in order to reduce the risks faced by their own staff. Risk transfer, in these circumstances, becomes a component of an operational risk management strategy where an organisation seeks someone else to carry out certain activities in a highly insecure context in order to reduce the risks to their own staff. This classical definition of 'risk transfer' has been the subject of much discussion in recent years and efforts are under way to address the inherent ethical duty of care failings that it can raise – especially where there is no clear assessment that indicates that local organisation staff are at lower risk than international organisation staff.

While it is sometimes easier for local actors to maintain access in volatile environments than international organisations, this should be properly assessed and agreed by both partners. International and local actors may face different risks and challenges in different contexts, including risks that they may transfer or create for each other through the partnership. In fact, by entering into a partnership, organisations automatically transfer risk, both intentionally and unintentionally. For example, in partnering with an international organisation to implement a high-profile programme, a community-based group may experience heightened risk due to the additional attention it can receive, including from local authorities and communities.

With this understanding, risk transfer is best understood as 'the formation or transformation of risks (increasing or decreasing) for one actor, caused by the presence or actions of another'.[47] This can extend beyond international–local partnerships, and includes relationships with donors and other actors, such as community-based organisations.

Good practice encourages partners to reflect on the impact a partnership can have on each other's exposure to particular threats and each organisation's capacity to address the risks before entering into a partnership arrangement.

47 GISF (2021) *Partnerships and security risk management: a joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Funding gaps

National organisations consistently receive insufficient, sporadic and project-based funding, which makes it difficult for them to develop the back-end systems and inputs needed to manage security risks effectively.[48] In the face of general funding scarcity and an extremely competitive funding environment, partnership budgets can fail to include security-specific budget lines or adequate core costs, while local actors can be incentivised to prioritise programme costs over security-related expenses when entering into partnership arrangements. Local partners may also feel compelled to accept higher levels of risk to secure funding. Knowing this, it is good practice for international organisations to systematically ensure that security funding exists for partners' budgets, either for assessed security costs or as a standard percentage of the overall funding provided.

Communication and trust challenges

There are many obstacles to communicating about security within partnerships, but the primary one is the failure to hold any discussion on security in the first instance. Communication around security issues too often defaults to due diligence checks of implementing partners or as one element of a broader 'capacity-strengthening' package driven by an international partner. Security focal points from both organisations may not be adequately involved in these initial discussions.

Security can be a sensitive topic and implementing actors may be disincentivised to speak honestly about their security challenges and any support needed out of fear of financial and reputational repercussions. Funding partners may fear legal liability if broaching the subject, as discussed above. Security discussions are also prone to challenges owing to a lack of common vocabulary; differences in understandings of security, risk and risk appetite; and power imbalances. Time is required to build and maintain trusting relationships, which short-term and project-based funding can further undermine.

3.5.3 Practical considerations

A strategic and policy-led approach to partnerships makes it easier for organisations to adopt an equitable security risk management approach. This aims to shift security-related conversations within the partnership from one-sided due diligence checks and 'risk transfer' to collaborative discussions on how to 'share risk', directly involving security focal points and relevant programme staff from all partners.

48 GISF (2020); GISF and Humanitarian Outcomes (2024).

GISF's *Partnerships and security risk management* guide offers a roadmap for implementing this approach, which is summarised in the following sections of this chapter.[49]

Before entering into partnership: a strategic approach and initial discussions

While there are many positive examples of informal collaboration between security focal points in partnerships arrangements, they are often not sustainable in practice. Without a clear strategic approach to why and when an organisation may seek partners, or how it will address security risk management within partnerships, security arrangements can be subject to individual staff members' preferences and biases, with any positive outcomes at risk of being lost when staff change roles.

Organisations that have developed policies around entering into partnership agreements and their responsibilities to their partners, as well as clearly stated security agreements, benefit from more strategic and better-balanced partnership arrangements that are more conducive to constructive security risk management discussions and mutual support. This strategic approach increases the likelihood that both partners benefit from the partnership, and reduces the likelihood of inadvertent and unaddressed risk transfer.

In practice, this includes ensuring that security considerations from focal points are incorporated in the strategic documentation of partnerships and related policies. Initial discussions can be incorporated into due diligence processes. If approached well, these discussions provide an opportunity for partners to collaboratively address concerns about risk transfer, assess security capacity and preparedness, and explore ways to support each other on security-related issues.

Case example: Beyond one-sided due diligence processes

One international NGO has started bringing its local security staff into the identification and contracting processes of local implementing partners. This has enabled the organisation to discuss security issues at the beginning of a partnership, and resulted in security becoming more than a due diligence 'systems review' within the partnership.

49 GISF (2021).

During this phase, partners should aim to assess how risk is being transferred between organisations and jointly find ways to address any challenges that arise – including identity-related risks stemming from external perceptions of the organisation and its staff. For example, if it emerges that a local community has negative perceptions about certain work an implementing partner is expected to do for its funding partner, the partners can discuss mitigating measures. This could involve reducing the visibility of those programme activities or modifying the project to enhance the security of implementing staff. See Table 3 for some key questions.

Beginning the partnership: agreeing on a security risk management approach

Soon after entering into a partnership or, if feasible and appropriate, before finalising the contract, organisations should aim to agree on how each partner can support the other on security-related issues arising in the partnership and in programme implementation.

GISF's *Partnerships and security risk management* guide provides a list of questions that can support these conversations and offers some ideas on the joint management of security risks between partners. A summary of key questions is in Table 3.

Table 3 Preliminary security risk management questions

Area	Questions
Duty of care	• What are the respective legal and ethical duty of care obligations of each partner? • Are these clearly explained in partnership documentation?
Governance and accountability	• Have both partners contributed to key decision-making opportunities regarding the programme, project, partnership and/or security? • Do both partners have suitable security risk management structures (including roles and responsibilities) in place to enable the partnership objectives to be met? • Does the partnership agreement include mention of security risks and their management? • Can the partners support each other, for example through the recruitment of dedicated security staff?

Area	Questions
Risk transfer	• How is each partner perceived by relevant stakeholders? • Could the organisational identity of one partner impact the other partner? • Does the partnership result in any new threats to either organisation? • Does the partnership change the impact or likelihood of any threat? If yes, is this positive or negative? • When exploring mitigation measures, can one organisation take particular actions to reduce the risk faced by their partner? • In conflict environments, how does the partnership interact with the dynamics of the conflict, and can steps be taken to be more conflict-sensitive?
Policies and principles	• Are the mandate, mission, values and principles of each organisation understood by both partners, and are both organisations comfortable with each other's work and approach to operations and security (e.g. do both parties agree with each other's position on humanitarian principles and safeguarding)?
Operations and programmes	• What are the security needs and expectations of each partner? • Do the partners have an agreed system in place to identify and monitor security risks faced by staff? • Do partners have security focal points who can speak to each other on security issues? • Do the partners agree on who is responsible for managing identified risks and how these positions should be managed and funded? • Is there a system in place to make both partners aware of security risks and changes in the risk environment (physical and online)? • Does each partner have enough resources (e.g. funding, time and staff) to manage security risks?
Inclusive security risk management approaches	• Does the security risk management approach of both organisations consider how staff members' identity can affect their vulnerability to threats? • How should sensitive identity topics, such as internal and external threats on the basis of sexual orientation or gender, be discussed by the partners? What are the comfort levels (accounting for cultural sensitivities)? • How can partners support each other to step out of their comfort zones to ensure effective security risk management for all staff?

Area	Questions
Internal threats and safeguarding	• How will the partners manage security threats that may arise from within their own organisations? • How are safeguarding concerns addressed within the partnership? • Are appropriate safeguarding reporting mechanisms in place?
Travel	• How should security risks resulting from travel related to the partnership be managed?
Awareness and capacity sharing	• How will partners identify security awareness and capacity-strengthening needs and jointly meet these (both for personal safety and security risk management)? • Can security staff from one partner provide advice, mentoring and technical support to security focal points in the other organisation, if this is needed? • Can partner staff access appropriate security training (internal and external to the partner organisations)?
Incident monitoring	• How should the partners share incident information with each other, if at all?
Incident and crisis management	• How will the partners collaborate/coordinate in the event of a crisis or critical incident affecting either organisation in the location where the partnership is active?
Staff care	• Do both partners have access to relevant insurance policies? If not, can either partner support the other in accessing relevant insurance? • Do both partners have staff care policies and procedures in place, including medical, mental health and post-incident support? • Can partners support each other with relevant staff care resources and activities (including making changes within the partnership to improve staff wellbeing, such as reducing workloads, flexible work hours and reducing administrative expectations)?
Security collaboration and networks	• Are there platforms in the relevant context that discuss security issues? If yes, do both partners have access and an equal voice in these platforms and networks in their operational areas, including security information-sharing platforms? • Can access to existing coordination mechanisms be improved for either partner?

Area	Questions
Compliance and effectiveness monitoring	• How should both partners review security risk management measures during the partnership?
Resources	• Have partners shared their respective resources on security risk management with each other? • Can access to existing resources be improved for either partner?
End of the partnership	• Will ending the partnership according to the contract (and financial timeline) have implications for the security of either partner? If yes, how should this be addressed?

Adapted from GISF (2021) *Partnerships and security risk management: a joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Finally, for a partnership to be equitable, it is crucial that both parties have a clear understanding of each other's attitudes to and tolerance of risk. Partners benefit from openly discussing each other's risk appetites and finding ways to align where there are strong differences – which can be quite stark in many of the contexts in which humanitarian programmes are carried out. Each partner's attitude towards risk should ideally be discussed at the beginning of a partnership and regularly revisited throughout the life of the partnership (which could match the schedule of partnership milestones). In some instances, it may be that agreement on risk thresholds cannot be reached or risks appropriately mitigated, and this can inform more strategic discussions on whether the partnership should go ahead or programmatic work should be modified.

▶ *See Chapter 1.1 for more on risk thresholds and programme criticality.*

During partnerships: identifying and addressing needs, gaps and challenges

Strengthening communication and operationalising principles

Proactive efforts can be made to improve communication between partners. This can mean ensuring that the right people are in the communication chain (which should typically include the designated security focal points of each partner); that the frequency and method of communication is the most appropriate and convenient for both partners; that communication is

transparent, honest and clear; and that staff adhere to key principles that aim to address and overcome inherent biases and build trust.

Partnership principles

In order to make partnerships more equitable, effective and secure, staff working on establishing and maintaining partnerships can consider some basic good practice principles:

- Equity – partners have equal rights, regardless of any power imbalances.
- Transparency – there is open and honest interaction between partners.
- Mutual benefit – both partners should benefit from the partnership, ideally beyond simply meeting the partnership objectives.
- Complementarity – partners each bring their own strengths and weaknesses to a partnership, complement each other and recognise that diversity can be an asset.
- Results-oriented – actions expected from partners should be realistic and focused on results.
- Responsibility – partners should take responsibility for their actions and avoid overcommitting or overpromising.

Source: GISF (2021) *Partnerships and security risk management: A joint action guide for local and international aid organisations* (https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Case example: Risk sharing in practice

A local Nigerian NGO approached its two international NGO partners for funding for the recruitment of a security officer. In addition to agreeing to provide funding for two new security roles in the local NGO, the international partners' security staff supported the recruitment process and provided the new recruits with inductions, bi-weekly support and monthly catch-up meetings. When discussing the benefits and challenges, international NGO security staff involved in the process agreed that buy-in from all partners was essential and ensured that ownership over security roles and decisions remained with each organisation. They agreed that, to share risk effectively, a key challenge is ensuring that international NGO security staff have the capacity to build relationships and provide the appropriate level of mentoring to local NGO security focal points.

Source: Christian Blind Mission (CBM) and Sight Savers International (SSI) (2022) *Sharing risk – a good practice example in the INGO sector* (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

Joint risk assessments and adapted security plans

Although still uncommon within the aid sector, joint risk assessments of programme activities provide both partners with a clear picture of the likely risks, and allow the implementing partner (and its staff) to voice concerns before carrying out the work. A joint risk assessment also allows for greater discussion on possible mitigation measures and ways in which each partner can support the other in meeting security needs and programmatic objectives. This process allows for clearer discussions around risk ownership and responsibilities within the partnership, as well as setting clear expectations from the start about what each organisation can bring to the partnership. A joint periodic review of the evolving risk picture is also advisable. The exercise can be an opportunity for partners to benefit from exposure to each other's perspectives and helps identify where adaptions may need to be made. For example, this could include reconciling one organisation's emphasis on documentation and written policies with another's reliance on verbal communication.

Depending on the circumstances, this joint risk assessment can culminate in shared security protocols. At the very least, these risk assessments should aim to inform each organisation's security plans and procedures. Regular communication between partners can help in addressing security concerns promptly.

Partners should be prepared for crises and critical incidents and ideally agree in advance the best way to manage them. Partners can consider which organisation would be best placed to respond in the event of a crisis or critical incident (e.g. logistics, access and expertise). Any support provided in these circumstances will usually need to be decided at a strategic level considering relevant legal and financial implications. However, being risk averse in this regard may not necessarily be the best option, as the reputational cost of not providing support during such an event (where an intervention would be beneficial and not cause more harm than good) may be more damaging than the possibility of legal liability. One international organisation that has recognised this has taken proactive steps to support their local partners with obtaining relevant insurance – something that can be very challenging for local organisations to obtain on their own.

Case example: Security risk management in partnerships

One international organisation has implemented several initiatives to better address security risk management issues and needs when working with partners. These include:

- Increasing the involvement of security staff in engagement with partners from the earliest discussions.
- Raising awareness among security staff of what partnership means and how to work together for common outcomes in a safe way.
- Creating (and sometimes co-creating) and sharing guidance, including tools.
- Offering a training 'menu' to partners.
- Increasing the number of partner staff in the organisation's own security training sessions.
- Supporting partners in managing incidents (in the form of technical advice).

Capacity sharing

Partners bring their own knowledge and strengths to a partnership and a discussion of these, as well as weaknesses and gaps, can lay the foundations of a stronger and mutually beneficial arrangement. Differences in approach should not be considered a lack of capacity. Partners should aim to agree on what is most needed in terms of support, for instance security training, and which formats work best. One international organisation created an online website that its partners can access for training on particular topics, including security-related content. Other organisations have promoted online platforms and training with their partners. Some international organisations have developed specific security training for their local partners, while others invite them to participate in the training they provide their own staff. It is important that all capacity-strengthening is relevant and beneficial to each partner, jointly agreed as needed, and sustainable so that it can support the long-term capacity of staff and organisations.

▶ *See Chapter 5.2 for more information on security training.*

Funding

Partners should aim to discuss security costs as early as possible, including the funding needed to strengthen back-end security systems. Partnership budgets should aim to contain security-related budget lines as a rule, while partners can ensure alignment of security cost requirements with assessed security risks. Longer-term funding needs should also be considered and discussed within the partnership, such as funding for training and medical and malicious act insurance coverage for staff most at risk. International partners can advocate with donors for adequate funding for their implementing partners, while donors themselves can demand greater consideration of the security needs of downstream partners.

▶ *See Chapter 3.3 for more information on funding security.*

Resource sharing

Partners benefit from proactively sharing security risk management resources and information within a partnership. Implementing partners may have greater insight into local security conditions, which they can share, while international partners may have greater access to coordination and information-sharing mechanisms, which they can facilitate access to. While this is often done informally, security resources should ideally be shared actively and regularly, be available online and offline (in a variety of formats where possible) and translated into relevant languages. Partners can support each other in engaging in security networks and information-sharing forums at local, national, regional and international levels.

Case example: Security coordination mechanisms

Local actors are significantly under-represented in coordination mechanisms led by international aid actors. Often, local actors are unfamiliar with the mechanisms or do not participate due to obstacles such as location and language. Organisations like INSO are taking steps to address this, offering membership to national registered NGOs and thereby allowing these actors free access to networking, information sharing and training. However, unregistered local humanitarian actors still face significant challenges in joining networks.

Advocacy and partnerships

Partnerships present opportunities as well as risks when it comes to advocacy. Common advocacy efforts between partners can result in an amplified voice, which can be useful for advocacy around security risk management (e.g. international partners advocating with donor governments for greater security funding for local actors). However, advocacy by one organisation can present security risks for its partners, for instance where a local government holds local partners in the country responsible for an international partner's advocacy efforts towards it. It is good practice to consider the impact that advocacy efforts can have outside the organisation, especially on partners, before moving forward. One international organisation in Myanmar has actively discussed advocacy messages with its implementing partners before going ahead in order to ensure that its partners are not only aware but also can discuss the possible consequences of the advocacy and any mitigation measures needed.

▶ *To learn more, see Chapter 2.2 on advocacy and security.*

Further information

Research and discussion

CBM and SSI (2022) *Sharing risk – a good practice example in the INGO sector* (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

EISF (2012) *Security management and capacity development: international agencies working with local partners* (https://gisfprod.wpengine.com/resource/international-agencies-working-with-local-partners/).

GISF (2020) *Partnerships and security risk management: from the local partner's perspective* (www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/).

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).

Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local-International partnerships (global report)* (www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships).

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

Guidance and resources

GISF (2021) *Partnerships and Security Risk Management: a joint action guide for local and international aid organisations* (www.gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

Global Database of Humanitarian Organisations (GDHO) (n.d.) (https://humanitarianoutcomes.org/projects/gdho).

4 Operational elements: processes and tools

4.1 Analytical elements

Good security risk management is built on solid analysis, and good practice holds that organisations operate more effectively and securely when they systematically evaluate risks. This chapter discusses the methodologies and tools used to conduct thorough risk analysis, to form the basis for informed decision-making and strategic planning. It underscores the importance of contextual understanding, enhanced by data-driven analysis, in developing robust security risk mitigation measures.

Context and risk analysis are not a precise science. Rather, they are a means to support organisations to increase their understanding and improve their decision-making by identifying the key questions to ask.

4.1.1 Overview

Listed below are the basic steps of an analytical process that security and programme staff have found useful (see also Figure 7). The specific activities undertaken within each step, detailed in subsequent sections, can vary in complexity and sophistication from organisation to organisation, depending on capacity and resources. It is important to remember that there is no one-size-fits-all, and the most appropriate model is the one that will be readily understood and consistently employed by staff at all levels. In general, organisations that opt for simplicity over complexity stand a better chance of their tools being used by staff.

Step 1: Context, threats and vulnerability analysis

- **Macro-context analysis.** Examine the broader context where the programming will take place, the conflict dynamics (if relevant) and the key actors.
- **Internal analysis.** Review the organisation's programme objectives, priorities, structures, geographical presence of staff, security risk management capacities and operating modalities.
- **Threat identification.** Identify potential dangers to the organisation's core assets (i.e. people), programmes, processes, property and reputation.
- **Vulnerabilities.** Identify the specific vulnerabilities (and strengths) of the organisation and its staff in relation to its programming and level of acceptance in the area.

Step 2: Risk identification and evaluation (risk assessment)

- **Risk identification.** List the plausible risks of working in the context based on the identified threats and the specific vulnerabilities of the organisation and its staff.
- **Risk analysis and evaluation.** Analyse the likelihood and potential impact of the identified risks. Rate them accordingly, from low to high, to determine priorities for mitigation measures and management planning.

Step 3: Risk mitigation and management planning

- **Mitigate identified risks.** Determine the measures needed to reduce the likelihood and/or impact of each of the risks. These will often be influenced by the organisation's security strategy (*discussed in Chapter 4.2*).
- **Address residual risk.** Reflect on any residual risk that may remain after all mitigation measures are implemented. Decide whether to accept, avoid or share it. This will be guided by the organisation's objectives, risk appetite and programme criticality.

Step 4: Monitor and review

- **Monitor and review.** Continuously monitor, review and adapt the risk assessment as necessary to ensure it remains relevant and effective.

This process can be documented and form part of security plans.

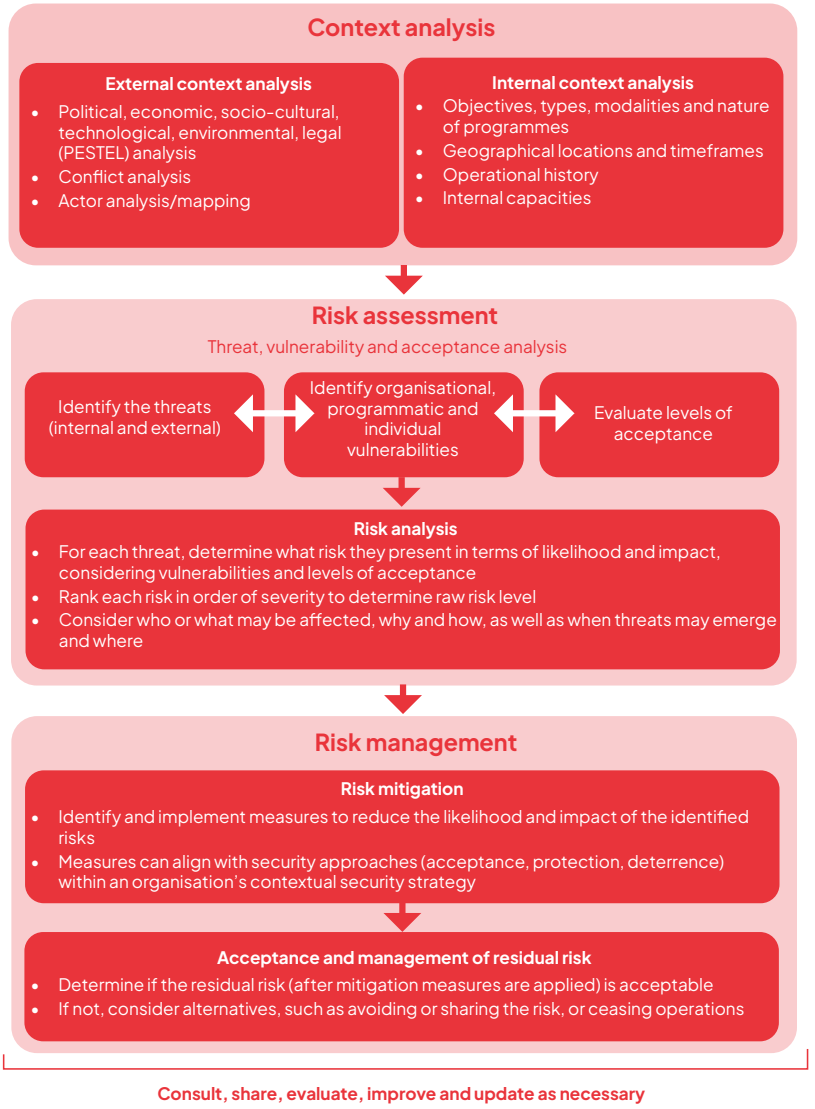
▶ *See Chapter 4.3 for more on security plans.*

To support this process, it is essential to continuously communicate risks, mitigation measures and their operational impact to all stakeholders while keeping staff informed of security changes and seeking stakeholder feedback. It is also important to regularly evaluate and update the organisation's security approach to ensure it remains relevant, reflects good practice and supports the organisation's ability to meet its objectives amidst changing conditions.

▶ *To learn more about communicating with staff, see Chapter 5.3.*

▶ *To learn more about monitoring effectiveness, see Chapter 3.4.*

Figure 7 Analytical process



Using a systematic approach to risk assessment is important because, while experience and intuition can play a critical role in understanding and responding to risks, relying solely on 'gut instinct' is not advisable. People's isolated experiences, invisible biases, individual perceptions and other subjective factors can often distort the view. Specifically, people tend to exaggerate rare, spectacular risks while downplaying frequent ones, overreact to immediate threats while discounting long-term dangers, and respond quickly to dramatic changes, but adapt slowly to gradual shifts (the 'boiling frog' or 'frog in the pot' syndrome). They can also struggle to assess unfamiliar risks, and overestimate widely discussed dangers.

A structured and disciplined approach can help to separate facts from perceptions and emotions, allowing the analyst to absorb more information for a fuller picture. It can also help teams arrive at a consensus, grounded in the available evidence. The individual(s) leading or coordinating the risk assessment process, usually security staff, should aim to ensure inclusivity. This involves gathering perspectives and information from all staff and considering risks through different lenses. This approach fosters a common understanding of risks and a shared responsibility for security measures. An example would be a risk assessment workshop where individuals with diverse personal profiles and roles come together to discuss the threats and vulnerabilities they personally experience.

In addition to generating a better understanding of risks as a basis for decision-making, a well-documented risk assessment can serve as an important managerial tool to keep track of changes in the operating environment, and provide a clear rationale for security investment. It can also provide a key performance indicator for programme activities, confirming that risks are being identified and managed during implementation.

4.1.2 Context, threat and vulnerability analysis

External context analysis

PESTEL framework

Analysis of the external context usually begins with examining the factors shaping the operational environment. Adopting the PESTEL framework can be a useful tool for this. In practice, this involves systematically evaluating each category to identify relevant risks and opportunities, and how these may impact the organisation and its staff. The categories are as follows.

- **Political.** The political environment, government stability, conflict dynamics, key power holders and contenders, political violence and government policies.
- **Economic.** Poverty, inflation, employment rates, currency stability, economic growth and inequality.
- **Socio-cultural.** Demographic trends, crime rates, community attitudes, norms, gender relations and intergroup dynamics that can influence acceptance and identity-based risks. This can include the history of aid in the area, and how the aid community and the organisation (if applicable) have been perceived by the local population.
- **Technological.** Technology, digital security and infrastructure stability, including internet and mobile coverage, digital literacy and technological limitations.
- **Environmental.** Climate-driven shocks and natural hazards, resource scarcity and competition and environmental regulations.
- **Legal.** Laws and regulations related to aid operations, including labour laws and compliance requirements. This can include the impact of legal factors on identity-based risks.

By using this framework, teams can better assess how external factors interact and influence their operations, leading to more informed risk mitigation efforts.

Conflict analysis

In addition to PESTEL, a more detailed conflict and violence analysis can help to illuminate sources of threat where armed conflict is occurring. Good conflict analysis does not focus just on where violence is visible. Violence can be preceded by tensions that may be less obvious: the 'deep divisions' and 'fault lines' in a society. These too must be explored and understood. Sometimes, multiple conflicts are interwoven. Tensions and outbreaks of violence in Iraq, for example, can turn on Sunni–Shia dynamics, the influence of ISIS, the competition for resources, Kurdish-Arab tensions or the legacy of the US invasion. Any and all of these can be a source of threat.

Several frameworks can support conflict analysis. However, this analysis does not have to be overly complex and can focus on answering some key questions, such as the following.

- **What are the visible and underlying causes of the conflict?**
  - Are there deep-seated grievances or divisions driving tensions (e.g. economic, political, social, historical)?
  - How do political structures, governance systems and economic conditions contribute to the conflict? Are there institutions that perpetuate exclusion or inequality?
- **Who are the key actors and stakeholders involved, and what are their interests?**
  - How do power dynamics and relationships between these actors shape the conflict?
  - What role do external institutions play in conflict dynamics (e.g. foreign governments and international agencies)?
- **What are the potential risks and dividers contributing to conflict escalation?**
  - Are there specific events or triggers that could worsen the situation?
  - What are the warning signs of a potential escalation?
- **What connectors or peacebuilding opportunities exist?**
  - Are there shared interests, cultural ties or local mechanisms that can reduce tensions?
  - What opportunities exist for peacebuilding or conflict mitigation through collaboration with local actors?
- **How might the organisation's interventions impact the conflict?**
  - Could the organisation's actions unintentionally fuel tensions, and how can staff ensure conflict sensitivity?
  - How can the organisation remain flexible and responsive to changes in the conflict environment, such as new alliances or unexpected violence?

Good practice involves regularly updating the conflict analysis to reflect changes in the situation, ensuring strategies remain relevant and responsive to evolving dynamics.

Actor analysis

Actor analysis, or actor mapping, focuses on the principal individuals and groups that potentially affect the security of an organisation and its staff – including staff members themselves. To remain relevant, such analysis must be ongoing, and initially will likely yield more questions than answers. It is an exploratory exercise that can proceed in three steps:

- identify and list all the relevant actors;
- understand their identities, motives, objectives and political/social positions; and
- analyse their relationships with each other.

In a conflict setting, relevant actors would include any armed groups and national and international actors participating in – or trying to influence – the conflict (including peacekeepers). Local actors could also include business owners, student groups, trade unions, landowners, militant religious or nationalist factions, the local media, local organisations and traditional leaders. Potentially relevant regional and international actors might be neighbouring powers, intergovernmental organisations, transnational corporations, diplomats, human rights organisations and diaspora groups.

The interactions between the various actors can be illustrated by lines drawn between them, representing different relationships – for instance, who is fighting, cooperating or competing with whom, and which groups fund or direct which others? A matrix can help staff visualise the relationships, updated as dynamics change (see Figure 8). Relationships can be categorised, for example as 'ally', 'friend', 'foe', 'complicated' or 'developing'. Different people may give different interpretations of these relationships, which should be considered in the development of the matrix. This exercise can also provide a convenient tool for briefing incoming staff. As the analysis deepens, it may become apparent that groups are not as homogeneous as they first appeared.

The potential threat actors to consider in the analysis include non-state armed groups, criminal actors, economic actors and government actors. It is important to recognise that these labels do not always apply with sharp distinctions; groups may overlap in objectives and motivations, and threat actors may change over time.

Figure 8 Simplified actor mapping example

Armed groups

Armed groups may encompass a large number of entities with different identities, motives and intentions, including extremist groups, organised criminal groups and politically motivated rebel groups fighting against a government. Understanding armed groups is vital to understanding how and why an organisation's presence and programmes might be manipulated or threatened. Depending on their power dynamics and ideology, armed groups may view humanitarian organisations as threats, proxy targets, political tools or sources of resources to exploit. Again, insights may come only gradually. For each identifiable armed group, organisations could assess their:

- Command and control structure – how organised and cohesive are the leadership and fighters?
- Contact points – who are the appropriate individuals for communication or negotiation?
- Ideology and worldview – what are their attitudes, beliefs and goals, if known?
- Public statements – have they made any remarks about aid organisations or operations?
- Past actions – what have they done, and how did they justify it?
- Symbols or mythology – do they use any notable symbols or narratives?
- Relationship with the local population – are they insiders or outsiders? Do they govern or provide services? The more abusive they are towards civilians, the greater the potential danger for aid organisations.

▶ *For more considerations on how to dialogue with armed actors see Chapters 2.1. and 4.2.*

Criminal actors

Criminal actors can see humanitarian organisations as lucrative targets for extortion, theft or kidnap for ransom, or as obstacles to their operations. To better understand these actors, organisations can consider:

- Organisational structure and hierarchy – who are the leaders and key members?
- Motivations and objectives – are they driven by financial gain, territorial control or illicit activities?
- Tactics – what methods do they use (e.g., extortion, kidnapping, cybercrime)?

- Relationships – how do they interact with local authorities and communities?
- Past incidents – what patterns of behaviour exist, especially towards aid workers and assets?
- Impact – what are the economic and social effects of their activities on the local economy and society?
- Communication channels – are there any potential interlocutors for negotiation, if necessary?

War economy actors

Many modern conflicts have been fuelled by 'war economies', including the illegal and quasi-legal trade in weapons, drugs, diamonds, oil, minerals and other materials. In areas where war economies are present, aid organisations could usefully examine:

- Resource importance – how critical are local resources to the war economy, and are alternative resources limited (making aid organisations more significant and vulnerable)?
- Geographical sensitivity – is the area important due to natural resources or strategic trade routes?
- Impact on recruitment – do aid programmes provide alternative livelihoods that may affect recruitment by armed groups or criminal enterprises?
- Economic impact of aid – does aid create tensions or dependencies that conflict actors might exploit?
- Environmental impact – could aid programmes worsen existing tensions or create new conflicts due to environmental effects?

Government actors

Governments can have a profound impact on aid delivery through their structures, political dynamics, legal frameworks and relationships with both local populations and aid organisations. It is beneficial to examine the stability, legal conditions and collaboration opportunities with government at different levels, as well as understanding:

- Government structure – what is the hierarchy, and who are the key decision-makers within relevant ministries or agencies in different locations?
- Political dynamics – how stable is the government, and what are the political interests that could affect programming?

- Legal frameworks – what laws and regulations apply to aid operations, and how are they enforced?
- Stance on aid – does the government support or resist aid efforts? Are there restrictions or conditions imposed?
- Corruption and accountability – are there issues of corruption within the government?
- Coordination – how does the government coordinate with aid organisations? Are there formal coordination mechanisms?
- Public perception – how is the government perceived by the local population?
- Security cooperation – does the government provide security for aid operations? If so, how?

► *See Chapter 2.1 for more information on engaging with authorities.*

Internal context

Internal context analysis looks inward at the organisation, its activities, assets and people. Assessment of the internal context can help staff gain a better understanding of the organisation as a whole, how its programme activities benefit the local population, and the level of acceptance it has in a given area, all of which feed into an understanding of the organisation's vulnerabilities and strengths. Some key considerations are:

- The organisation's mission and programme objectives.
- The type and nature of programme interventions.
- Geographical locations of project teams and assets.
- Operational history in the area, if any.
- Implementation modalities.
- Timeframes of activities.
- Internal organisational capacities to manage risks.

When establishing the internal context, security staff can collaborate with programme staff responsible for managing and implementing programme activities, the operations team and sub-office workers to gain as much insight as possible.

Threat identification and assessment

Following the context analysis, the next step is to identify specific threats in the operational environment and the specific vulnerabilities of the organisation and its staff.

A threat is any event, action or entity with the potential to cause harm to personnel, programmes or assets, or hinder the achievement of aid objectives. Security threats stem from a variety of sources, including crime, conflict and violence, while threats to staff safety include accidents, illness and natural hazards.

Internal threat sources

Threats can emanate from inside the organisation as well as outside. Security incidents perpetrated by aid workers against colleagues can take various forms, including harassment, discrimination, bullying and sexual violence. Theft, fraud and breaches of confidential information can compromise organisational integrity and resources, leading to staff insecurity. Physical violence and psychological abuse by colleagues, including tactics like gaslighting and manipulation, are also risks. Internal perpetrators can be motivated to cause harm for a number of reasons, including:

- The target's identity (for example their gender, ethnicity or sexual orientation).
- The perpetrator's personal circumstances, including any personal grievances, their family history, personality and behaviours.
- Permissive organisational environments.
- External cultural and societal factors.

▶ *See Chapter 1.2 for more details on internal threats.*

▶ *See Chapter 7.7 for more on sexual violence risks and a deeper discussion of how to handle internal perpetrators.*

External threat sources

In looking at external threat sources, it can be helpful to develop threat descriptors based on various actors and categories of events. Examples may include threats relating to:

- Crime (homicide, theft, carjacking, burglary, assault).
- Sexual violence (rape, assault, abuse).
- Detention and arrest (roadblocks, checkpoints).
- Abduction (kidnap for ransom, hostage situations, extortion).
- Combat-related threats and remnants of war (shooting, shelling, airstrikes, bombs).
- Information, communications and technology (cybercrime, online harassment, disinformation, data leaks, hostile surveillance).
- Civil unrest (demonstrations, protests, mob violence).

Threats can also emanate from environmental factors, such as economic ones (recession, inflation, supply chain disruption) as well as natural hazards (floods, earthquakes, epidemics).

► *For a more detailed discussion of some types of threats, see Part 7.*

Once the threats have been identified, it is important to understand how, when and why each might occur, and who/what it can affect (in terms of people, programmes, assets, property and reputation, for example).

Gathering threat information

The information used for threat analysis can come from a range of sources, including local authorities, staff members, community leaders, business owners, taxi drivers, local and international media and human rights monitors. Some of these sources may be well informed and willing to share what they know, while others may be ill-informed or may give a deliberately distorted picture. Private security companies can also provide information and analysis on security conditions and potential threats. This can be helpful for macro analysis, though it tends not to give the kind of day-to-day detail organisations may require at the area level.

There are a variety of methods for collecting information about potential threats in the operating environment, including direct interviews with stakeholders and an analysis of documentation, such as a review of past organisational reports (including from peer organisations), NGO databases, coordination forums, UN agencies and local police. Open sources, including social and mainstream media, can also be valuable. Quantitative analysis of past incidents can help identify

trends and high-risk areas. Visits can also offer a chance to gather first-hand observations of the situation in the location.

Information should be assessed for reliability (source authenticity and trustworthiness) and validity (consistency and confirmation by other independent sources). Using a matrix to rank the reliability and validity of sources can enhance the quality of threat analysis.[50]

In any setting, it is possible for different individuals and groups to view threats differently depending on their day-to-day experiences and interactions with threat actors. Focus group discussions, interviews and participatory assessments can help organisations gather more nuanced information.

Vulnerability and acceptance analysis

After completing the threat assessment, the next step is to assess the organisation's vulnerabilities: the degree to which staff, properties and assets are exposed to the threats.

An organisation's vulnerability can be influenced by:

- Image and acceptance level of the organisation.
- Type and nature of the programming.
- Location of staff and property.
- Level of exposure of staff and property.
- Value of assets/property.
- Impact of programme interventions in the area.
- The organisation's internal capacity to manage security risks.
- Staff training, awareness and compliance with security measures.

Understanding individual staff vulnerabilities

Personal vulnerabilities, encompassing both immutable aspects of identity and manageable factors like behaviour, collectively form an individual's personal risk profile. Not all identity characteristics or vulnerabilities are visible, for example health, sexual orientation or financial stability. Vulnerabilities are only relevant when they overlap with a specific threat, and security staff should aim to understand and address vulnerabilities in this context.

50 For an example, see RedR UK, Insecurity Insight and EISF (2017) *The security incident information management handbook* (https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools).

As part of a person-centred approach to security risk management, organisations can systematically evaluate how different identity factors – such as gender, sexual orientation and ethnicity – affect an individual's vulnerability to internal and external threats. An inclusive risk assessment can encompass a range of factors influencing individual vulnerabilities linked to the interplay between staff members' intersectional identities, their roles within the organisation, the context and internal and external threat factors. This ensures that risk assessments are inclusive, and should ideally involve input from diverse staff members to capture a broad spectrum of experiences and perspectives.

Case example: Inclusive risk assessments

One organisation divides their security risk assessment into indirect threats ('where you are') and direct threats ('who we are, what we do'). This allows staff to use external data to develop a baseline security level, that is then complemented by a deeper analysis of risks that staff may experience when carrying out their work. Under this framing, what may be a low-risk country based on context can be revealed as an internally high-risk location due to factors such as low community acceptance.

▶ *To learn more about the person-centred approach, see Chapter 1.2.*

Understanding organisational and programme vulnerability

Internal context analysis can help identify organisational and programme-specific vulnerabilities. Perceptions of the organisation, its role, mandate and mission can affect its vulnerability to threats. Faith-based organisations, whether or not they are proselytising as part of their mission, may have different risks in religious contexts than secular organisations. Similarly, international organisations associated with particular countries, or national organisations associated with particular areas or ethnic groups, may be targeted for political reasons. UN agencies may find it difficult to escape being identified with the UN as a political actor, despite their humanitarian mission. Certain programme activities, such as reproductive health services or aid that focuses on marginalised communities, can entail risks due to how these programmes may be perceived by local communities. Governments can take a negative view on where and with whom

organisations are working if they deem it counter to their interests, particularly if they see it as directly or indirectly supporting opposition groups.

Organisations whose programming spans the 'nexus' of humanitarian, development and peacebuilding activities will likely face a more complex threat landscape as their agenda extends beyond providing humanitarian services into potentially sensitive areas of political and societal interest.

Programme analysis involves understanding the organisation, what it aims to do where and when, and, most importantly, why.

- **Why**. Why is the programme needed and how critical is it to the people it serves? How important is it to the organisation's mission and identity?
- **What**. What are the key activities and what operational modalities are involved (e.g. travel, distributions, logistics chain, working in local facilities, working at the community level)? How have activities been perceived and received by the community in the past?
- **Who**. Who are the target population, donors, local and broader stakeholders? Who are the programme staff and what intersectional identities will need to be considered?
- **Where**. What are the programme locations and other areas where staff will be or pass through?
- **When**. What are the programme timelines, and do they coincide with periods of expected heightened insecurity?

The above questions can help reveal areas of vulnerability and indicate the level of acceptance the organisation has gained.

Evaluating the level of acceptance of the organisation within the community and among stakeholders is crucial, as a lack of acceptance can increase risks and hinder programme success. This analysis can examine stakeholders' influence, their perceptions of the organisation and its staff and current engagement levels, identifying risks and actions to maintain or strengthen acceptance where necessary.[51]

▶ *See Chapter 4.2 for more on acceptance analysis.*

51 For an example acceptance analysis template, see GISF (n.d.) 'Acceptance analysis template - xlsx'. *2. Acceptance analysis.* NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

4.1.3 Risk analysis

Once an organisation has identified threats and vulnerabilities in a particular context, the analysis can turn to risks. Risk is a multidisciplinary subject with different meanings in different situations, involving a wide range of known and unknown possibilities. When it relates to security, risk is a combination of two factors:

- the likelihood of encountering a threat; and
- the consequences that would result.

The most critical risks to address are those that are likely to occur and/or have the potential to cause major harm, while highly unlikely and/or low-impact events will usually rank lower in priority.

Risk assessments should be collective and collaborative, bringing diverse staff together, including programme and operations staff, to ensure that a diversity of perspectives, lived realities and identity profiles are considered.

Assessing likelihood

The likelihood assessment evaluates how probable it is that an adverse event will occur.

Estimating the likelihood of a security threat is generally guided by trend analysis and information from both internal and external sources. This information is used to determine the potential frequency of the event. Likelihood can be evaluated by using a five-point scale, as illustrated in Table 4.

Table 4 Qualitative assessment of likelihood

Rating descriptor	Likelihood descriptor
Certain/imminent (5)	The event occurs on a regular basis, is sure to happen, or is already happening
Highly likely (4)	The event/threat has a very high chance of occurring
Likely (3)	The event has happened before and has the potential to occur again
Moderately likely (2)	The event rarely occurs
Unlikely (1)	The event is unlikely to occur

Assessing impact

Evaluating impact involves understanding the potential consequences to people, programmes, processes, property and reputation. In other words, it is the estimation of the harm that could be caused by a threat. Impact can be classified in two ways:

- Direct loss – the immediate harm caused by the event, such as death or injury of staff, vehicle damage or loss of assets.
- Consequential loss – far-reaching impacts such as delays, time lost, cost of medical treatment and psychosocial support provided to affected staff, disruption of operations and office closure.

A single incident can have both direct and consequential loss.

As with likelihood, impact assessment can use a five-point scale (see Table 5).

Table 5 Impact assessment

Impact rating	Impact descriptor
Extreme (5)	Exceptionally grave impact such as death, mass casualty, loss of operations, programme suspension, office closure
High (4)	Major impact such as serious physical or psychological injury to staff, loss of humanitarian access, significant financial loss, reputational damage
Moderate (3)	Moderate impact such as non-life-threatening injury, loss of assets, staff and programme restrictions, financial loss, some reputational damage, non-critical illness
Low (2)	Low impact such as loss of or damage to an organisation's assets, minor injuries, minor disruption
Negligible (1)	Insignificant impact

Risk matrix

To produce the risk level for each threat identified, the organisation can then:

- Take the list of threats identified during the threat assessment.
- Estimate the likely impact if the threats were to happen, and the likelihood that these threats will occur.
- Define the overall raw (i.e. not yet mitigated) risk level.
- Plot the threats according to their risk level (likelihood x impact) in a risk analysis matrix or risk analysis map.

Figure 9 presents a simple four-level matrix used in risk assessment to evaluate and prioritise risks based on their likelihood and impact. Each combination of likelihood and consequence corresponds to a risk rating, which can help organisations visualise and prioritise risks according to their severity. The shading represent overall levels of risk, ranging from low (light) to extreme (dark).

Figure 9 Risk matrix example

Impact / *Likelihood*	**Negligible (1)**	**Low (2)**	**Moderate (3)**	**High (4)**	**Very high (5)**
Certain / imminent (5)	Medium	High	High	Extreme	Extreme
Highly likely (4)	Medium	Medium	High	Extreme	Extreme
Likely (3)	Low	Medium	High	High	Extreme
Moderately likely (2)	Low	Low	Medium	High	High
Unlikely (1)	Low	Low	Low	Medium	Medium

Risks can be sorted by a number ranking, or simply as 'high', 'medium' or 'low'. High risks usually require immediate attention and robust mitigation measures. Moderate risks may need regular monitoring and targeted mitigation measures. Low risks could perhaps be managed with baseline measures, such as standard operating procedures and occasional reviews. This detailed analysis and evaluation process can help an organisation prioritise its resources and efforts effectively, focusing on the most significant risks and ensuring that all potential threats are adequately managed.[52]

52 For example templates, see GISF (n.d.) *3. Risk assessments.* NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/risk-assessments-2/).

Context risk ratings

Many organisations manage security on the basis of 'risk ratings' or 'security levels' assigned to specific locations. Typically there are three to five levels, ranging from low to high risk. Many different levels can exist within a country or even a city. The levels inform many administrative and operational decisions, including programme criticality, security measures, travel risk management oversight, security staffing, security budgeting and HR policies.

When establishing these context risk ratings, a similar risk assessment process can consider the threat environment, the vulnerability of the organisation and its staff in that location, and the importance of that location to meet overall programme objectives.

This tiered approach helps establish security requirements for different locations, and ensures that resources are allocated efficiently and that the most critical areas receive the necessary attention to mitigate potential threats. While this approach is usually used for locations, it could be applied to other relevant categories as well. For example, it may be helpful to identify which roles in the organisation are the highest risk and outline security requirements for those staff members (e.g. specialised training).

▶ *See Chapter 3.1 for more on security requirements.*

Risk mitigation

The risk assessment can provide a roadmap for the organisation to allocate sufficient resources and develop specific risk mitigation measures that correspond with identified risks.

The security measures used to mitigate risk will typically involve – and be influenced by – a combination of approaches that make up an overall security strategy for an organisation in a specific context.

▶ *See Chapter 4.2 for more on the different security approaches and developing a security strategy.*

Risk mitigation (or treatment) measures are designed to reduce risks by lowering vulnerabilities and enhancing capacities through reducing likelihood and impact.

- **Reducing likelihood.** Identifying and applying specific actions to make incidents less likely to occur, such as establishing standard operating

procedures (SOPs), setting rules such as curfews and speed limits, using convoys and buddy systems and training staff on skills to avoid threats.

- **Reducing impact.** Once an incident has occurred, the impact can be reduced by protective and readiness measures such as having access to reinforced shelters or saferooms, equipping facilities and vehicles with first aid kits and fire extinguishers, preparing critical incident management and contingency plans, and having insurance and staff care resources such as counselling services.

Mitigating measures should reflect the risk assessment in terms of likelihood and impact. If a threat is high impact but low likelihood, it may be more appropriate to focus on efforts to reduce the impact rather than investing more in reducing the likelihood. That said, it is advisable to address both as far as possible. Once risk mitigation measures have been identified, these will need to be implemented and funded.

Finally, as with context analysis, the risk assessment will need to be a living document if it is to remain relevant and useful. A key aspect of this process is tracking and analysing security incidents and other relevant information to identify patterns or trends that could indicate evolving risks. Risk assessment and mitigation measures feed into, and are usually documented in, security plans.

► *See Chapter 4.3 on security plans and arrangements.*

4.1.4 After risks are assessed and mitigated

Once a risk has been 'treated' by mitigating measures, ongoing risk management involves determining how to handle the residual risk that remains as some risk will usually be present even after implementing measures to reduce it. How an organisation approaches residual risk is usually shaped by its mandate and objectives, the criticality of its programming and the organisation's defined risk appetite. There are at least three potential avenues an organisation can take.

- **Accepting the residual risk.** Deciding to accept certain levels of risk if they are within the organisation's risk tolerance. This is often appropriate for mission-critical or lifesaving work where the potential benefits outweigh the risks.

- **Avoiding the residual risk.** Taking steps to avoid risk by altering plans, processes or behaviours to eliminate the threat entirely: for example, relocating operations away from high-risk areas or discontinuing non-critical activities.
- **Sharing the residual risk.** Engaging a third party, such as a partner organisation, to share the risk by taking on programming activities in a way that optimises effectiveness and security for both, and upholds duty of care.

In cases of very high risk, the pivotal question is whether to remain present and operational, or to cease activity and withdraw. This can be broken down as follows:

- Is it necessary and appropriate for the organisation to remain? Does it have the capacities (financial and competencies) to manage the security risks?
- If not, can these capacities be developed or brought in quickly enough?
- Once financial and human resources are in place, can enough staff and management time be devoted to managing security risks?

If the answer is 'no' to any of the above, organisations should think seriously before deciding to go ahead, at least until the situation improves or adequate capacities are available to manage the risks. There are valid alternatives to a physical programming presence, including channelling funding or other resources through organisations that are better placed to securely operate in the setting in question.

4.1.5 Thinking outside the risk matrix

Current thinking around risk analysis questions whether some organisations have taken the systematic approach too far, suggesting it has become overly complex, arcane and regimented to the point where it is divorced from intuition and experience. Like any set procedure, there is also a danger that it becomes a box-ticking exercise instead of a tool to support decision-making.

As mentioned previously, one advantage of working within a framework for security risk evaluation is that it brings organisational consistency in the response to risk, and can be used to trigger a set of actions without hesitation or lengthy discussion. However, as a management tool it may also give a misleading sense of robustness and predictability, and it is important to understand the limitations of this approach:

- Incomplete information and the difficulties involved in correctly interpreting a complex reality may make it difficult to decide whether to move to a different state of alert, and in any case identifying the right security rating is not the same as implementing the plan.
- Risk level classifications can sometimes be too broad to capture gradients of threat or categories of those at risk in the same location.
- Real-life situations do not always gradually worsen or improve – a situation can suddenly deteriorate, jumping across multiple levels.
- Different organisations operating in the same location may interpret the same situation differently, and consequently put themselves in different security ratings with correspondingly different security measures.
- Evacuations and relocations in moments of crisis usually require interagency collaboration, which may be complicated by different appreciations of the risk, while the fact that some organisations relocate/evacuate while others do not may change the risk and increase vulnerability for those staying behind.

The other concern is that focusing attention and resources on the most likely high-impact risks, which is the logical endpoint of the exercise, can hinder people's ability to envision and consider far less likely, but potentially catastrophic, risks. An organisation that is only prepared to contend with a list of the likeliest risks, this argument holds, may be less flexible and resilient in the face of events that can never be predicted. Some organisations are adopting a process called 'horizon-scanning', which is essentially group brainstorming about improbable events that, if they occurred, would have a severe impact. The exercise can prompt staff to think creatively about a broader range of threat scenarios and come up with response strategies that could potentially address a variety of events.[53]

Decision-making under uncertainty is a constant in complex humanitarian environments, where information is scarce and the situation is dynamic and unpredictable. Effective decision-making requires balancing between rapid response and comprehensive analysis, often employing both analytical and naturalistic (intuitive and experienced-based) decision-making approaches.[54] Building in horizon-scanning exercises as part of the threat assessment can

53 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).

54 For a more detailed discussion see Cole, A. and Olympiou, P. (2022) *Risk management & decision making under uncertainty during the Afghanistan crisis 2021.* GISF (https://gisfprod.wpengine.com/resource/risk-management-under-uncertainty-during-the-afghanistan-crisis-2021/).

prevent formulaic approaches that, in the worst case, reduce risk assessment processes to mere budgeting tools.

However, having a systematic, structured method for risk analysis does not necessarily call for a heavy bureaucratic process or a technically complex exercise. Rather, it should be simple enough that all staff can meaningfully participate, and light enough that it can be done (and redone as necessary) in a short period of time. It is important for organisations to adapt the risk analysis process to their organisation, considering needs and capacities.

4.1.6 A simplified approach

Risk assessment processes can often seem complex and overwhelming. While this chapter has provided detailed methodologies and good practices for risk analytics, for organisations with limited time or staff capacity it may seem unrealistic to systematically implement all of the steps outlined.

In such cases, simply reviewing and reflecting on the following key questions can help guide risk analysis and mitigation. The point, of course, is not to achieve the perfect risk analysis process, but to maximise situational understanding and evidence-based decision-making to the extent possible.

Key risk analysis questions

- **What is the external context?**
  - What political, economic, socio-cultural, technological, environmental and legal factors are relevant?
  - Who are the key actors (armed groups, criminal actors, government elements) affecting security, and how do they interrelate?
  - Is there active conflict and, if so, what are the causes? Who are the actors and what is their relationship to the organisation and each other?
- **What is the internal organisational context?**
  - What are the organisation's objectives, structure, capabilities, programmes, staff and locations, and how do these relate to the external context?

- **What are the main threats in the operational environment?**
  - What are the internal and external threats to the organisation?
  - How, when and why might each threat occur, and who/what would it affect?
- **How vulnerable is the organisation to identified threats?**
  - What vulnerabilities exist for staff and the organisation, especially considering intersectional identity factors, programme assessments and acceptance levels?
- **What is the likelihood of the threats occurring?**
  - What is the likelihood of identified threats happening?
  - Which threats are most likely?
- **What are the potential impacts of identified threats?**
  - What is the potential impact of each identified threat?
  - Which threats have the most significant consequences, and who/what could be most affected?
- **What mitigation measures can be implemented?**
  - Which threats are the most concerning and require risk mitigation (usually those that are more likely or have a more serious impact)?
  - Which actions can reduce the likelihood and/or impact of identified threats?
- **What will the organisation do about residual risks?**
  - Will the organisation avoid or accept and/or share any residual risk left over once mitigation measures have been put in place?
- **What low-likelihood but high-impact risks need more attention?**
  - Which risks require scenario planning or further discussion due to their potentially severe consequences despite their low likelihood?

When assessing risks, it is helpful to consider who or what may be affected (including identity-based factors), why and how, as well as when threats may emerge and where (considering both the physical and digital spheres).

Further information

Research and discussion

Cole, A. and Olympiou, P. (2022) *Risk management & decision making under uncertainty during the Afghanistan crisis 2021*. GISF (https://gisfprod.wpengine.com/resource/risk-management-under-uncertainty-during-the-afghanistan-crisis-2021/).

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).

Guidance and resources

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/).

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

GISF (n.d.a) *1. Context analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/1-context-analysis/).

GISF (n.d.b) *2. Acceptance analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

GISF (n.d.c) *3. Risk assessments*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/risk-assessments-2/).

RedR UK, Insecurity Insight and EISF (2017) *The security incident information management handbook* (https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools).

4.2 Developing a security strategy

An organisation's security strategy in a particular operational context comprises a balance of approaches and the specific measures it decides to take. These are informed by the risk assessment process, together with the organisation's principles and values. This chapter introduces the three broad, overlapping security approaches that can shape a security strategy: acceptance, protection and deterrence.

4.2.1 Security approaches

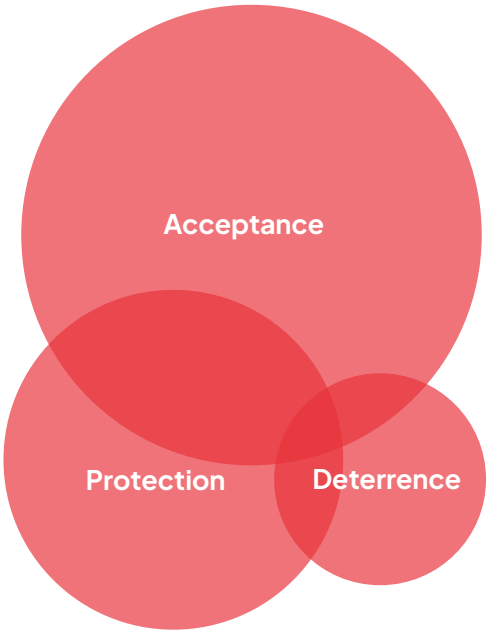
The concepts of acceptance, protection and deterrence each constitute a range of security options and actions, from 'soft' to 'hard'. As discussed previously:

- Acceptance measures attempt to reduce or remove threats by increasing the acceptance (the political and social tolerance) of an organisation's presence and its work in a particular context.
- Protection measures aim to reduce vulnerability to the threat but do not affect the threat itself[55] – this is often called 'hardening the target'.
- Deterrence measures aim to deter a threat with a counter-threat, such as the use of force (the classic example is armed guards).

Although acceptance, protection and deterrence are sometimes seen as separate strategies – each their own corner of 'the security triangle' – in practice, an organisation will usually choose a mix of options from each, depending on the operating environment. In different settings and as risks evolve, it may be appropriate to shift the emphasis from one type of measure (or overarching approach) to another. Rather than a static triangle, therefore, it may be more useful to imagine overlapping and interactive spheres, which can vary in emphasis depending on the context, risks and organisational strategy (see Figure 10).

55 Many security professionals, and previous editions of this GPR, used the word 'protection'. Note, however, that some security professionals use the term 'protective' (as in 'protective approach' and 'protective measures') to make a clear distinction between security risk management measures for staff, and protection as a type of humanitarian intervention focused on at-risk communities.

Figure 10 Example combination of measures in a security strategy



Given their principles and values, many humanitarian organisations view acceptance as the most appropriate and effective overarching approach and make it the foundation of their security strategy in a particular location (i.e. with most risk mitigation measures designed to increase acceptance, while actively avoiding any measures that may negatively affect perceptions and acceptance). This may mean, in some contexts, that an organisation decides not to use any deterrence measures at all, if doing so is perceived as not in line with the organisation's principles, values and acceptance approach.

Acceptance measures are not effective against all threats, which is why a combination of measures is often necessary. In environments where lawlessness or violence is pervasive or where armed actors have few incentives to negotiate, acceptance measures may have limited effectiveness on their own. However,

adding other types of measures does not necessarily mean abandoning an acceptance-led approach. On the contrary, the optics of adding visible protective measures, for example, may require more outreach and other active acceptance measures. The effectiveness of any approach will also be influenced by what other aid organisations are doing.

Protection and deterrence measures are not necessarily more effective in all cases and can bring their own problems. Protection measures focus attention on the organisation as a potential target and, unlike acceptance, do not address those who pose the threat. It can also lead to a 'bunker mentality', which can result in a restrictive operational model and a greater distance from target communities, all in order to reduce risk by insulating the organisation, its staff and assets. This makes it harder to develop relationships with others, which in turn makes it harder to get information about the environment and to communicate effectively with local interlocutors.

Deterrence measures – the least used among humanitarian organisations – have obvious downsides. If organisations display force, for example by driving with armed escorts or hiring armed guards for their offices, it is harder to convey an image of neutrality and non-violence.

A good security strategy needs a flexible combination of these measures, which may mean choosing one overarching approach that can guide the decision on what measures to prioritise. As a basis for any programming activity, it is good practice to cultivate acceptance and good relationships with the local population and their leaders, as well as relevant state and non-state actors. In more insecure environments with identified general risks to aid organisations, certain protection measures are usually advisable, particularly against crime. In highly insecure contexts, where there are significant risks to the organisation, deterrence measures may be necessary if this is the only way to protect staff and continue providing critical assistance, sometimes referred to as the 'principle of last resort'. If acceptance is the main approach, protection and deterrence measures can be adapted to maintain acceptance. Acceptance measures can be used to complement protection and deterrence risk mitigation measures.

Different measures have different resource implications. All carry a financial cost. Acceptance is perhaps the hardest to measure in financial terms but may require considerable staff time and possibly new programme initiatives, such as media outreach. Protection equipment carries a direct financial cost, while protection procedures (for example curfews or always driving with two cars) can add to

the budget by restricting operational capacity. A deterrence approach can have both small and large resource implications, which may be difficult or impossible to back out of in the long term (e.g. investing in armed protection).

4.2.2 Acceptance

Acceptance is often a broader organisational approach that focuses on fostering genuine relationships with affected communities and stakeholders while upholding core humanitarian principles. This approach is often seen as fundamental to providing legitimacy and consent for effective programme implementation. An acceptance approach also allows humanitarian organisations to distinguish themselves from other actors, such as military forces or private sector service providers.

In security risk management, acceptance is often understood as reducing or removing potential threats by cultivating and maintaining relationships with relevant stakeholders and gaining their 'consent' to operate in a particular location. In reality, 'consent' may not be the most appropriate concept to measure acceptance by. In practice, acceptance can be more helpfully understood as a continuum, ranging from accepted (most secure) to targeted (most insecure):[56]

- accepted
- tolerated
- rejected
- targeted.

Challenges to acceptance

The challenges to – and limitations of – acceptance are numerous. The following are some of the most prominent.

- **Funding.** How an organisation is perceived may be linked to where it gets its funding. The suspicion that those who provide the money control the aid organisation can create significant problems, particularly if the donor in question is a party to the conflict or is perceived as having a political agenda.

56 To learn more, see Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management.* Save the Children Federation (https://acceptanceresearch.wordpress.com/acceptance-toolkit/).

- **Principled humanitarian action.** In some contexts, both national and foreign governments may not want aid organisations negotiating or even communicating with non-state armed actors, even if this is necessary to undertake principled humanitarian action and access crisis-affected populations. Governments may penalise such negotiations, for example using counter-terrorism legislation. Organisations that accept funding with counter-terrorism clauses attached will need to ensure that all reasonable steps are taken to ensure compliance without compromising the humanitarian mission.
- **Advocacy.** The pursuit and preservation of acceptance may make it difficult for organisations to speak out about violations of international humanitarian law or human rights abuses as this can negatively affect relationships with various stakeholders. Organisational leadership benefit from having a structured approach to balancing advocacy efforts with security risk management concerns. (*See Chapter 2.2 on advocacy for a more detailed discussion.*)
- **Harmful information.** The implications of misinformation, disinformation, malinformation and hate speech for aid worker security are a growing area of concern and study. (*See Chapter 6.2 for a more detailed discussion on the challenges posed by harmful information.*)[57]
- **Proliferation and fragmentation of armed groups.** In many contexts the proliferation and fragmentation of armed groups is making it more difficult to determine who is in control of what territory, as well as who is in charge within an organisation (i.e. will negotiations with one representative be honoured by the rest of the group?). Some organisations have invested significant resources in monitoring armed groups to understand their internal structures and shifting patterns of territorial control.

Key components of active acceptance

Acceptance cannot be assumed; it must be actively forged and diligently maintained. 'Active acceptance' measures include strategic outreach to a wide range of stakeholders; developing staff skills in social, political and interpersonal relations and communications; and designing and disseminating core messages regarding the organisation's mission, objectives and programmes. Key components of an active acceptance approach include:

- Working with programme staff to integrate security risk management into programme design.

57 For a discussion on how technology can impact acceptance, see Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' in GISF (ed.) *Achieving safe operations through acceptance: Challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

- Establishing and maintaining relations with key stakeholders, including armed actors. This can include engaging with national, regional and international actors, where relevant.
- Gaining acceptance from local populations (e.g. through meetings and socialising).
- Managing communications.
- Monitoring perceptions and public sentiment.
- Managing perceptions of staff and the organisation.

These are discussed in more detail in the following section.[58]

Programme integration

The ability of an organisation to meet people's needs in a transparent and accountable way is often critical to how it is perceived. Acceptance is widely recognised as connected to effective and responsive programming that meets the needs of a community. Community participation, consultation and local partnerships are often key elements of effective programming. However, even if programmes meet the needs of affected people, they may adversely affect specific actors or change political, economic and social power structures. Insofar as good programming is an essential component of acceptance, acceptance cannot be assumed from good-quality programming alone.

The connection between effective programming and gaining/maintaining acceptance should aim to be explicitly referenced in programme planning activities, included in programme plans, needs assessments and budgets, and incorporated into programme monitoring and evaluation tools.

Interacting with key stakeholders

Once key stakeholders have been identified and their respective positions, influence and disposition analysed, organisations can approach those who formally or informally exercise meaningful influence on whether an organisation can operate securely in a given environment. These may be friendly, unfriendly or neutral towards the organisation and can be identified in the actor analysis. National, regional and international actors must be considered alongside local stakeholders, as acceptance from these is becoming increasingly more important for effective humanitarian action.

▶ *See Chapter 4.1 for more on actor analysis.*

58 For a more detailed discussion of an active acceptance approach, see Fast et al. (2011).

It is important to assess the influence that each party has – in some situations having the acceptance of key influencers might be sufficient if it is not possible to secure the acceptance of all. Relying on staff from the area or using a respected intermediary (such as a religious or community leader) to reach out to other stakeholders on an organisation's behalf can support acceptance.

Building a relationship with key stakeholders usually requires more than rare, brief formal meetings. Messages can be conveyed not only in meetings but also through the type of meeting and how it takes place. Cultural customs should be followed and respected. Slowing down, taking time to meet and talk to people, explaining, listening, socialising and generally showing basic politeness and respect can all be important in securing acceptance.

Formal agreements, for instance with the government or with influential groups, can be useful in that they provide official recognition and explicit agreement on specific issues. With regard to security, agreements can spell out detailed responsibilities, including the procedures to be followed and a point of contact should security problems arise. Operational staff may wish to carry a copy of the agreement with them (in the relevant language) to facilitate access or dialogue. It is important to bear in mind that written agreements do not have the same value in every social environment, and other cultural practices may be more appropriate. Formal agreements can also be problematic, for example if they are valid for only a limited period of time, if they draw attention to areas where authorities may be inappropriately seeking to regulate or impede aid organisations' activities, or if they consume more staff time than they are worth. Formal agreements may also not be recognised across all levels of a group/entity. These factors should be considered before entering into formal agreements.

Non-state armed actors

Organisations working in an area under the de facto control of an armed group are likely to have to signal their presence to them and obtain assurances that their work is acceptable and that staff will not be harmed. Questions to consider when interacting (or considering interacting) with these actors include:

- What is the relationship between the armed group and the local population?
- What is the armed group's relationship with the organisation's staff?
- What is the command structure and state of discipline? What are the aims and objectives of the armed group?

- How might dialogue and negotiations with the armed group affect relations with others (including authorities)?
- What requests or demands (for example paying 'taxes' or getting daily 'permission' to operate) might be made, and how should the organisation respond?

Understanding these dynamics and risks requires a proactive capacity to analyse them. It will often make sense to work with other aid organisations to pool capacities and enable a common approach and common red lines (non-negotiable limits) when interacting with non-state armed actors.

▶ *See Chapter 4.1 for more discussion on armed groups as part of an actor analysis.*

Local populations

If there is a high level of acceptance, members of the local community may make suggestions as to how risk can be reduced, and in some cases may provide critical information and warnings to the organisation. Their influence, however, should not be overestimated, and in some circumstances communities may not be in a position to meaningfully reduce security risks at all. They may be powerless to influence other actors, may overlook or misjudge new threats, or may benefit more from supporting another actor.

There is a difference between mere tolerance of an organisation's presence and programme and true acceptance. People may accept an organisation's presence only because they are in desperate need, or may use aid as one source of support but may not feel an active responsibility for the organisation's wellbeing. Listening and responding to what people want, treating them with respect, acting transparently and being accountable may deepen relationships and encourage a greater level of acceptance. These relationships may even override the material dimension. An aid organisation can find itself unable to provide an adequate level of assistance or periodically even any assistance at all, and yet remain accepted based on the quality of the relationship.

Managing communications

For all stakeholders, communications need to be clear and consistent. An organisation and its staff should know and be able to explain – in succinct, easy-to-understand language – who they are, why they are there, what they want to do and how they relate to others. A simple question and answer sheet for staff can be helpful.

In the case of international and federated organisations, the need for consistency extends to aligning messaging globally. While certain communications may be adjusted slightly for different audiences, the overall message should aim to be the same, whether from head office or at a project site.

Public statements should reflect an organisation's values, principles and mandate and be contextualised for local understanding, as well as being mindful of the impact on local perceptions.

Critical public statements about local authorities require careful consideration. Key factors to weigh include the necessity of public disclosure, when to inform the subject, the phrasing and substantiation of claims, and the method of release.

▶ *For a more detailed discussion, see Chapter 2.2 on advocacy and security.*

Managing perceptions of staff

How staff are perceived can influence perceptions of the organisation as a whole. Identity-based characteristics play a role in this and can present both strengths and vulnerabilities, depending on local perceptions of those identity characteristics.[59]

▶ *See Chapter 1.2 for more discussion on identity-based factors and perceptions.*

Appearance and behaviour are also important. Personal appearance can carry important social and political meanings, and inappropriate behaviour can cause resentment and aggravate existing suspicions and tensions.

Respect for social and cultural norms (e.g. customs around dress, alcohol and interpersonal relations) can improve perceptions of staff and the organisation. Not all customs can be known or respected by those who are new to the context, but mistakes can be more easily forgiven if accompanied by a polite, composed and respectful attitude, or a clear position as to why customs are not being followed.

59 For a discussion of the benefits of recruiting a diverse and inclusive staff for acceptance, see Williams, C., Kinch, P. and Herman, L. (2021) 'Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Religious norms should also be considered and respected wherever possible; faith-based organisations may need to be extra careful about their image and activities.

Managing perceptions of the organisation

It is important to consider how the organisation and its activities are perceived. Are programmes what the local community most want and need? Some programming may not be considered a priority or may be negatively perceived by certain segments of the community. How do stakeholders who are not benefiting from the programme view the organisation and its staff? Are these stakeholders in a position to negatively impact acceptance among others, obstruct programmes or harm staff?

Understanding these issues entails listening to people and adapting accordingly. Even if a programme has wide acceptance within a community, it may still aggravate other stakeholders. This is true in virtually all sectors: a food aid programme may anger local traders by cutting into their profits; providing free health services may draw patients away from paid-for clinics, frustrating local health officials; and recording protection threats against the population may anger those responsible for the violence.

Another consideration is the exit strategy. Organisations may run good programmes but find that poorly executed exit strategies undermine the goodwill that had developed over the period of the programme. This means that they may struggle to gain acceptance in future.

Capacities and competencies for acceptance

Acceptance has practical implications, in terms of human resources, finances and administration. An active acceptance approach requires staff with certain key competencies. These can include:

- The ability to map key actors and establish a wide network with stakeholders.
- A thorough understanding of the mission and values of the organisation.
- Strong relationship-building and negotiating skills.
- Fluency in the local language and excellent communication skills.
- The ability to analyse changing political and security conditions.

Effectively applying an acceptance approach requires leadership from senior staff, who will need to have not only the requisite skills, but also sufficient time relative to their other responsibilities.

Acceptance is not cost-free. There are operational costs, including:

- Staff time, including hiring additional staff with security, outreach or media responsibilities.
- Training staff on how to communicate the organisation's mission and values, as well as cross-cultural communication and diplomatic and negotiating skills.
- Additional travel (vehicles, fuel, staff time) may be required to meet stakeholders.
- Translation of organisational materials or messages into locally appropriate formats and languages.
- Paying for the use of radio and television and other media, where necessary.
- Additional time required during the design phase of a programme.
- Communication materials, such as flyers.

These costs should be identified in the programme design and integrated into the budgeting process.

► *See Chapter 3.3 for more information about funding security.*

Pursuing an acceptance approach may also require adjustments to administrative or legal standards within the organisation, such as in the following examples.

- Although suppliers are generally chosen based on price and quality, an acceptance approach may require spreading contracts over different sectors of the local population so that people feel that the benefits are shared fairly. Likewise, it may be a good idea to buy locally, even if a non-local provider offers better value for money.
- The organisation may choose to adjust its recruitment procedures to contract a balance of diverse profiles (considering ethnicity and whether people are from the local area, for example).

Monitoring perceptions and measuring acceptance

There is no simple way of knowing how an organisation is perceived and whether (and why) it is accepted. It can be a positive sign of acceptance if relevant stakeholders:

- Publicly commit to accept responsibility for staff security.
- Share accurate security-related information with the organisation (e.g. warn that someone has been asking around about the organisation or that a certain threat is likely).
- Actively cooperate with or support the organisation's activities.
- Allow access (e.g. armed groups let organisation staff through checkpoints to reach programme areas).
- Help to secure the release of an abducted staff member or recover stolen assets.
- Acknowledge that the organisation has made a positive difference in people's lives.
- Apologise if members of a group do the organisation harm.

Acceptance can be the result of one staff member's strong relations in a particular location or setting. Organisations should be aware of this, and the potential implications if this staff member leaves the organisation, or perceptions of that individual change.

Acceptance may also diminish over time as people's needs and expectations evolve. Once a situation has stabilised, new aspirations can arise. Organisations should strive to continually monitor attitudes among local populations and key stakeholders to gauge levels of acceptance and any changes that might interfere with access and security.

A lack of acceptance, however, may have nothing to do with the organisation itself and cannot necessarily be improved by its efforts; it may, for instance, be a rejection of the concept of humanitarian action as a whole.[60]

60 For a more detailed discussion on the limitations of acceptance, see Daudin, P. (2021) 'Acceptance under stress: old recipes for new problems' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

How to monitor and measure acceptance – some ideas

- A good understanding of the context and relevant stakeholders is a foundational element of monitoring acceptance.
- Introduce acceptance analysis as part of existing ways of working. This GPR presents it as a step in the security analysis process. Assessments of acceptance could also be integrated into security audits or community forums.
- Levels of acceptance can be gauged against objective criteria/indicators, such as the frequency of meetings with key stakeholders and the level and nature of interaction with key actors. Incident data can be useful but should not be the only indicator.[i]
- It may be helpful to break down relevant stakeholders and determine the level of acceptance of each, and outline useful information and key follow-up actions.[ii] It may be also beneficial to break down the acceptance levels of different actors in the location in question: the aid sector as a whole, the organisation and specific programmes and teams.[iii]
- Ways to gather information to inform this analysis include:
  - monitoring social media posts and mainstream media
  - conducting focus groups and consultations
  - undertaking periodic perception surveys
  - establishing feedback mechanisms
  - documenting the nature of informal conversations.
- Once acceptance levels are determined, these can be fed into a dedicated action plan or incorporated into risk mitigation measures and other activities. Unpacking the different factors that can influence perceptions, and determining the level of control the organisation has over these, can guide action (e.g. staff behaviour vs the political motivations of armed groups).

[i] For more examples of indicators, see Fast et al. (2011).

[ii] See, for example, GISF (n.d.) *2. Acceptance analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

[iii] See, for example, Billaudel, R. (2021) 'Measuring and improving acceptance: ACF's experience and perspectives' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Monitoring and analysing acceptance levels is a largely subjective exercise. This subjectivity can be managed by encouraging multiple individuals to participate in the evaluation process and having them share concrete examples to explain their impressions, using multiple sources of information, and using objective and standardised indicators across teams and locations.

4.2.3 Protection

Protection measures aim to reduce vulnerability. This can be achieved either by hardening the target or by increasing or reducing its visibility.

Hardening the target

Physical assets and procedures can reduce the likelihood of a threat getting near the target, or reduce the potential impact of harm on the target. In practice, this could mean:

- Site security equipment, such as installing lighting and alarm systems, erecting perimeter walls or installing metal gates and metal bars on windows (*see Chapter 7.2 for more details*).
- Asset protection, such as safes for cash and valuable equipment and vehicle alarms.
- Protection procedures such as controlling visitors' access, vehicle access and parking arrangements, and hiring guards to patrol locations and warn if there are intruders.
- Using armoured vehicles, personal protective equipment (PPE) and blast film on windows.
- Training staff on digital security (*see Chapter 6.2 for more details*).
- Driving in convoys, or arranging staff accommodation so that residences are grouped close together.

Strength in numbers can be effective but may not necessarily stop a determined attacker and could be counter-productive if greater numbers of casualties are the aim, or if another organisation is targeted and others become collateral victims. Likewise, while communications equipment is usually necessary, visible and expensive equipment may attract unwanted attention. Light and sound (e.g. movement-sensitive floodlights outside a building) can give some advance warning of an attack, allowing staff to take evasive action (get into a safe room, slip out) or call for assistance. Again, however, these devices may not prevent an incident.

Low-profile/low-visibility programming

Low-visibility programming has become increasingly common among aid organisations, especially when acceptance is determined not to be a viable approach. It involves removing organisational branding from office buildings, staff, vehicles and residences. It can also involve the use of private cars or taxis. In very high-risk environments, anything that might link staff to an organisation – organisation identity documents, mobile phones, computers – may be 'sanitised'. Staff likely to stand out from the local population may be moved to another location. In extreme low-profile postures, aid recipients may not be made aware of the source of assistance.

Another tactic of a low-visibility approach is to use removable logos for vehicles in areas where visibility is discouraged. Knowing when to display a logo, and when to take it off, demands a very good, localised and dynamic risk assessment. It is important to bear in mind, however, that removable magnetic stickers can easily be stolen and used by others to impersonate the organisation.

A low-profile, low-visibility approach can make programming more complicated and can distance the organisation from sources of information that might otherwise enhance its security. It might also lead to suspicions and misperceptions of what the organisation is doing, undermining acceptance. It is a difficult approach to maintain if the organisation is seeking wider recognition for its work from the public or from donors. Organisations generally do not see a low-profile approach as a permanent way of operating; rather, it is often viewed as exceptional and time limited. It may also be adopted at the start of a programme, and then gradually moderated as operations increase.

4.2.4 Deterrence

Deterrence involves posing a counter-threat: essentially, discouraging would-be attackers by instilling fear of counterforce or other serious consequences. Armed protection is the strongest form of deterrence used by aid organisations. There are other potential deterrents, however, and this section covers them briefly before going on to an in-depth examination of armed protection in humanitarian operations.

Forms of deterrence

Legal and diplomatic leverage

There are legal protections for aid workers under national and international law. Unfortunately, legal deterrents are not always effective. Some aid organisations may secure some leverage from the backing of foreign donor governments, particularly in negotiating access or resolving administrative problems with national governments, but their influence will be limited, and close interaction with donor governments can undermine the appearance of independence and neutrality.

Suspension of operations or withdrawal

In the face of certain threats or after security incidents, organisations have temporarily suspended their aid programmes or threatened to do so. The continuation or resumption of the programme is then made conditional upon the resolution or amelioration of the problem. Anecdotal evidence suggests that this tactic does not always work very well, and that organisations often resume their programmes despite no noticeable improvement, which can undermine their credibility and any such similar threats in the future.

The following are circumstances under which a suspension or threat of suspension may be effective:

- If it is not perceived as punishing people not linked to the causes of insecurity and who are not in a position to improve security.
- If an influential section of the population or local leadership/authorities can be mobilised on the organisation's behalf.
- Where organisations are prepared to maintain the suspension until the situation is satisfactorily resolved, and will not annul the decision too quickly because of internal or external pressure.
- Where other organisations do not undermine the action by stepping in to fill the gap – a common front ideally needs to be established before operations are suspended.

Unless the incident is very serious, a selective suspension (e.g. in a given location or for a given period) or the gradual reintroduction of services may provide more room for manoeuvre. A total suspension tends to create a difficult all-or-nothing situation.

▶ *See Chapter 4.3 for a practical discussion of the security implications of suspensions and withdrawal.*

Informal affiliation

Another deterrence option is to affiliate informally with influential local actors. In this scenario, an attack on the organisation might be implicitly perceived as an affront to these actors. This option needs to be approached very cautiously as it could undermine the organisation's humanitarian principles and its acceptance with other stakeholders, and could even result in the organisation becoming hostage to the protection of the powerbroker in question.

Armed protection

Humanitarian organisations do not normally use armed protection. However, there may be exceptional circumstances where it becomes necessary in order to enable humanitarian action, such as for humanitarian convoys entering major combat environments or where authorities demand it as a condition for access. That said, while armed protection might provide a measure of security and protection for humanitarian aid workers in the moment (though they can also do the opposite and draw fire), it can also complicate efforts to sustain humanitarian access in the long term. In other words, the practice undermines principled humanitarian action. IASC guidelines offer several reasons to avoid using armed escorts for humanitarian convoys because of the counter-productive implications in the long term.[61]

The relationship between armed protection and humanitarian action is fraught. Although virtually all aid organisations at one time or another have used some form of armed protection, it is often considered anathema, and discussions about it are highly sensitive. Cooperation with an armed actor – including a UN-mandated force – can lead local, national and international actors, as well as the population, to associate humanitarian organisations and aid recipients with the political and/or military objectives of that armed actor. This could potentially undermine the actual and perceived neutrality, impartiality and independence of the humanitarian organisation and the broader humanitarian community, as well as its acceptance. The impact of armed protection on acceptance is not always straightforward and can vary depending on the context and other influencing factors.[62]

61 IASC (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys).

62 For a discussion on this, see Jourde, J. (2021) 'Private security contracting and acceptance: a dangerous match?' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

While this section provides a more systematic framework for considering the matter, it is not intended as an argument for the use of armed protection but rather an exploration of potential benefits, risks and challenges. Before deciding whether to use armed protection, it is advisable to consider the pros and cons in the specific situation and explore all possible alternatives.

The following questions can be considered when deciding whether to use armed protection:

- Under what circumstances does the organisation permit the use of armed protection, in principle?
- Do the benefits of using armed protection in this context outweigh the risks?
- Are there serious concerns about how to manage armed protection, and can these concerns be overcome?
- How will the use of armed protection affect perceptions of the organisation particularly, and aid organisations generally, and impact levels of acceptance among key stakeholders?
- What are the local culture and practices relating to the use of armed protection? (This can affect how its use is perceived and accepted.)

At every step in the line of reasoning, it is possible to arrive at the conclusion that armed protection may not be appropriate. Bear in mind also that the need to consider armed protection at all may indicate that the threshold of acceptable risk has already been crossed, and the real decision that needs to be taken may be to withdraw or not begin programming. If this threshold has not yet been reached, or if armed protection could reduce the risk to a more acceptable level, then three major areas come into play in thinking through the decision: principles and ethics, context and management.

Issues of principles and ethics

Some argue that armed protection is against the basic principles of humanitarian action. This position tends to be based on ethical or long-term operational considerations. The ethical argument holds that humanitarian action is never compatible with the use of force. From an ideological perspective, an organisation may refuse armed protection because its use, as a matter of principle, contributes to the ongoing production and distribution of arms.

The long-term operational consideration is that, whereas armed protection might be justifiable in a given context, it may also erode the overall image of humanitarian action worldwide and may therefore lead to increased insecurity elsewhere or in the future. According to this line of reasoning, resorting too quickly or too often to armed protection undermines global efforts to increase respect for international humanitarian law and independent humanitarian action.

There are also practical considerations. Armed escorts make aid work much less flexible in terms of movements, as permissions and escorts often have to be organised in advance. Making movements more predictable may increase an organisation's vulnerability to attack, particularly if escorts are not fully trustworthy.

Arguments in favour of the use of armed protection hold that it can be acceptable as a last resort, and when people's survival would be at risk if humanitarian and other assistance were curtailed.[63] In some contexts, the use of armed protection to facilitate the provision of aid may be a function of the state exercising its obligations under national and international law or government policy.

Another major consideration concerns who benefits from armed protection:

- Is it only the aid organisation and its staff, or can the protection provide wider public benefits and enhance public security?
- Will the use of arms and armed guards – perhaps recruited locally – have a pacifying effect on the local situation, or will it increase tensions?
- Is it contributing to the 'privatisation' of security, whereby only those who are able to pay can obtain security?
- Is it indirectly putting others at risk by making them soft targets in comparison? It is important to consider what effect, if any, it has on the broader security environment.

Even if the use of armed protection is deemed necessary and legitimate, it may not be ethical or practical to pay for the service from private contractors, groups or individuals. Protection from a state or internationally mandated police or military forces may be provided free of charge in some contexts, but not always. Following experiences with protection rackets among Somali militia guards in the 1990s, some aid workers argued that aid organisations should never pay

63 UN and IASC (2008) *Civil–military guidelines & reference for complex emergencies.* UN Office for the Coordination of Humanitarian Affairs (OCHA) (https://digitallibrary.un.org/record/697614?ln=en&v=pdf).

for armed protection. The reality is that most have done so when they judged the circumstances required it. It is also sometimes a legal obligation in some contexts.[64]

Dependence on support from an armed actor can also make it extremely difficult or impossible to operate without such support in the future, undermining the sustainability of humanitarian operations. The provider of armed protection may develop a financial interest in maintaining the service. Additionally, the sudden cessation of armed protection can expose a humanitarian organisation as a soft target.

One organisation's decision to use armed protection has implications for others, as it can influence the image and perception of all humanitarian organisations, and therefore potentially affect acceptance and relationships more widely. This is a topic that merits structured interagency reflection and discussion. While generally rare among NGOs, armed guards and/or armed escorts are commonly used by UN agencies operating in contexts deemed high risk, such as Afghanistan, Iraq and Yemen. In many contexts, this has led to divergent security postures between UN and NGO humanitarian actors. During clashes in the Gambella region of Ethiopia in 2022, UNDSS recommended the use of armed escorts for humanitarian deliveries. Some international NGOs were later alarmed to discover that their local teams in Gambella had acted on this recommendation.

Questions of context

Beyond questions of principle, ethics and risks to an organisation's acceptance, a set of further, context-specific questions can be posed when deciding on the use of armed protection.

- *What are the threats and who are the targets?*

Deeper analysis can shed light on the source of the threat, the target and the motives of potential perpetrators. Important distinctions can be made between threats related to site security and movement security, and threats specifically to the aid organisation (its personnel and assets) and more generally to affected populations. Even where armed protection appears justified, it may not provide a reasonable deterrent, or may increase the risk. For example, if burglars suspect that a resident has a firearm, they may turn violent if surprised in the act. If road bandits see an armed convoy, they may shoot before robbing it. Who is the target is also an important consideration. If armed protection is provided by government forces or a particular faction, the organisation may become a

64 Stoddard, A., Harmer, A. and DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations*. HPG Report 27. London: ODI (https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/).

legitimate target in the eyes of the armed opposition. There is also the risk of accidents from 'friendly fire' or mishandled or malfunctioning weapons.

Maintaining the distinction between the organisation and its armed protection

Aid organisations can consider the following actions to distinguish or distance themselves from armed protection:

- Ensure armed actors protecting convoys travel in separate vehicles.
- Prohibit weapons inside the organisation's premises or vehicles.
- Avoid wearing clothing (including colours) that resembles that of armed forces.
- Refrain from using military assets (e.g. trucks, helicopters); repaint and re-mark if unavoidable.
- Exclude armed guards from compounds unless absolutely necessary.
- Use armed bodyguards only for targeted threats like kidnapping or assassination, applying 'close protection' when needed.

Whether these steps actually help to maintain a perceptual distinction and allow the organisation to retain some part of its civilian and non-combatant image often depends on the specific local context.

► *Who is being protected?*

In dangerous environments, organisations tend to think about measures that will enhance their own security. It may be helpful to consider whether and how security could be improved in the area more generally. For example, armed guards in a refugee camp might be deployed in a way that protects not only organisation staff, but also refugee women at risk of sexual assault when collecting water and firewood. A system might be developed whereby the armed guards of several individual organisations patrol the neighbourhood and therefore increase the security of all. Where a UN peace operation is present and has a mandate to protect civilians, troops may be deployed to areas that are dangerous both for aid workers and for the local community.

► *Who is providing protection?*

It is also important to consider who is providing the armed protection. Potential sources include national military actors, national police, an armed resistance group, UN peacekeepers or police, local militia, private security companies and armed guards directly on the organisation's payroll. In some circumstances, an organisation not opposed in principle to the use of force may find that none of the potential providers is acceptable and effective, leaving the organisation the choice between operating without armed protection or withdrawing.

Example questions when choosing an armed protection provider

- What is the political position of the provider in a given conflict? Can the organisation be seen as taking sides if it associates itself with a particular actor?
- What is the provider's public image and reputation?
- How important for the provider is the extension of protection to an aid organisation compared with its other objectives? The provider may have another agenda (for instance engaging the enemy or capturing a criminal) that in critical moments may override concern for, or even jeopardise, the organisation's security.
- How professional is the provider? Are guards well trained, reasonably compensated, provided with functioning equipment, well instructed, supervised and disciplined?
- How much management control does the organisation need or want? Having more direct authority over the providers of armed protection allows for greater control, but also makes the organisation directly accountable for their behaviour and actions.
- What are the provider's 'rules of engagement' on the use of force and where does liability sit should force be exercised and injuries incurred?

► *See Chapter 2.1 for a broader discussion of private security providers, including some more detailed questions about code of conduct.*

Questions of management

A key managerial question relates to the rules of engagement (i.e. when force can be used and to what degree). The basic rule is usually that force can only be used to protect life when clearly threatened, and as long as the threat persists. In other words, lethal force can only be used in defence and not, for example, to shoot a burglar, even an armed one, who is fleeing and no longer constitutes an immediate threat. What constitutes an immediate threat to life and wellbeing should be worked through in concrete terms, imagining different scenarios.

Rules of engagement should also be clarified for the protection of assets. While an organisation's instinctive preference may be that no force should be used when only assets are at risk, is it acceptable to do nothing while a warehouse is emptied or all the food in a convoy is stolen by armed actors, especially if there are people that really need and are dependent on those supplies? Organisations should aim to be very clear at what point and in which scenario engagement is acceptable.

Case example: Rules of engagement in practice

One international organisation has used unarmed guards from a private security company in the Democratic Republic of Congo and South Sudan. The company also has an armed response unit with either its own armed guard or an embedded armed police officer. While the organisation primarily uses unarmed guards, discussions with the private security company also covered key questions including the rules of engagement in the event this armed response unit was summoned.

Another important management aspect is to agree procedures and approaches for a number of possible scenarios, including what to do when a visitor refuses to be searched or insists on bringing in their own armed guards, and how far to go in the pursuit of fleeing robbers or attackers.

For instances where armed protection is sought, agreement may need to be reached on:

- Who provides the weapons (this is normally the provider of the personnel).
- What type of weaponry the guards will use (e.g. pistols, single shotguns or machine guns).
- Who is responsible for providing the ammunition and for checking that the weapons are well maintained and properly registered.
- Who is responsible for the provision of additional equipment, such as clothing and torches for guards.
- What vehicles, if any, armed guards have access to – armed guards do not always come with vehicles and decisions may have to be made about if and when they can use the organisation's.

Command and control work both ways: if an organisation puts itself under the protection of an armed actor, it may be expected to abide by the armed actor's rules. For example, suddenly leaving a convoy, speeding ahead or driving off may not be accepted by the security provider.

In a multinational peacekeeping force, different national militaries tend to have different traditions and cultures, including with regard to command and control, rules of engagement, and what is considered appropriate or excessive use of force. Detailed in-depth consultation with commanders at different levels may be required to ensure a common understanding. Different commanders may have different views, and it can be helpful to have a detailed written agreement with a senior commander to manage relationships across different levels. It is advisable to monitor changes to make sure that any replacements are fully briefed.

► *To learn more about civil-military coordination, see Chapter 2.1.*

Summary of key managerial questions

Key management questions to consider include:

- Are the policies, procedures and management competences necessary for handling this relationship available within the organisation and the location in question?
- What are the necessary contractual stipulations?
- Who maintains command and control, and who has authority and responsibility for what?

- Who in the aid organisation makes the decision/approves the use of armed protection?
- Will the armed guards always be present or only at certain times or in certain places?
- How are tenders drawn up and bids assessed from private security providers?
- What inquiries can be made concerning the professionalism and integrity of a potential service provider?
- Who are the guards answerable to, who has the authority of command and who is in charge of discipline?
- Where external security forces provide armed protection, what is the authority of their commander versus that of the organisation?
- Who determines the rules governing the use of deadly force, and who ensures that guards have fully understood them?

Policy

Organisations benefit from having an organisation-wide policy on the use of armed protection. Important points to consider include:

- Clarification of the organisation's position regarding the use of armed protection in principle.
- The conditions that could justify the use of armed protection, for instance during the evacuation or relocation of staff in periods of extreme insecurity (this can include references to programme criticality and the consequences of using armed protection).
- What alternatives have been considered to address risks, and if armed protection is truly the last resort.
- The key considerations and risks (legal, reputational and physical), both for the organisation concerned and for others, when choosing potential providers, and how they are to be evaluated.
- The terms that need to be agreed between the organisation and the provider.
- The organisational procedure for decision-making and periodic review.

- The obligation to accompany the use of armed protection with increased communication efforts to explain its rationale – that is, how it can support other security approaches, especially acceptance.

Sample policy

Under the policy of one organisation, armed protection can be considered when:

- large numbers of lives are at risk;
- the threat is related to widespread banditry, not political;
- the provider meets relevant standards;
- the deterrent can be effective; and
- the use of armed protection is authorised at the appropriate organisational level.

A policy on armed protection is not the same as a policy on private security companies, even though private security companies are often the providers of armed protection. An organisation might contract private security companies for other purposes (e.g. risk assessments or security audits) and other types of actors can also provide armed protection. The use of either should be guided by established policy.

► *To learn more about private security providers, see Chapter 2.1.*

Further information

Research and discussion

Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Bamber-Zyrd, M. (2023) 'ICRC engagement with armed groups in 2023' *Humanitarian Law & Policy*, ICRC (https://blogs.icrc.org/law-and-policy/2023/10/10/icrc-engagement-with-armed-groups-in-2023/).

Daudin, P. (2021) 'Acceptance under stress: old recipes for new problems' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

GISF (2021) *Achieving safe operations through acceptance* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Stoddard, A., Harmer, A. and DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations*. HPG Report 27. London: ODI (https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/).

Williams, C., Kinch, P. and Herman, L. (2021) 'Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Guidance and resources

Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management*. Save the Children Federation (https://acceptanceresearch.wordpress.com/acceptance-toolkit/).

GISF (n.d.) 'Acceptance analysis template - xlsx'. *2. Acceptance analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

United Nations and IASC (2008) *Civil–military guidelines & reference for complex emergencies.* UN Office for the Coordination of Humanitarian Affairs (OCHA) (https://digitallibrary.un.org/record/697614?ln=en&v=pdf).

4.3 Security plans and arrangements

Once an organisation has identified and evaluated the risks, it can make plans to manage them. A security plan is where these risks are documented along with their corresponding mitigation measures. This chapter identifies good practice in creating security plans, with a focus on two major elements: standard operating procedures or SOPs (how the organisation will mitigate the threats identified in the risk assessment); and contingency arrangements (how the organisation will respond to disruptive and potentially high-risk events and situations).

4.3.1 Security plans

The security plan serves as the foundation of security risk management at the programme implementation level. Depending on the context and the risks, a security plan may apply to an entire country, a specific geographic location or even, occasionally, an individual project.

Inclusivity in the planning process – involving a diverse group of staff with different roles, backgrounds and personal profiles – is preferable to individual planning, as it brings to bear collective knowledge and experience and promotes broad ownership of the final product. Good practice in planning also includes following up with periodic reviews to adapt the plan as the environment changes.

Components of a security plan

Security plans differ across organisations, reflecting specific organisational needs and policies and the context. The major components of a security plan can include the following (adapted from the EISF (now GISF) *Security risk management: A basic guide for smaller NGOs*):[65]

1. **Critical information summary.** A one-page cover summary of key details for quick reference, including emergency numbers and important procedures or rules, such as curfew or check-in times.
2. **Overview.** The purpose and scope of the plan, the responsible party, a statement of the organisation's mission and security policy (including risk appetite and threshold), and dates of the plan's creation, last review and next review.

65 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/).

3. **Current context and risk assessment.** A synopsis of the operating environment in a defined timeframe, including conflict dynamics, if relevant, and the identified threats, risks and risk ratings.
4. **Security levels.** Phases based on risk indicators and required actions.
5. **Roles and responsibilities.** The names of people and positions with responsibilities for security risk management.
6. **SOPs.** Clear and concise security procedures for prevention and response based on assessed risks and covering key areas like cash handling, communications, site security, health and safety, information security, personal conduct, travel security and vehicle safety.
7. **Health and safety measures.** Specific SOPs and other measures to protect staff from health threats, accidents and stress.
8. **Human resources.** Summaries of policies for recruitment, background checks, contracts, confidentiality, inductions and role risk assessments.
9. **Security briefings.** A list of the topics covered and information provided to new staff/visitors and training requirements/expectations.
10. **Incident reporting.** Definitions, procedures, responsibilities, reporting structure and format.
11. **Crisis management and contingency plans.** Crisis management structure, plans, teams and activation rules for crises and critical incidents, as well as contingency plans for relocation, hibernation, evacuation, disasters and medical emergencies, for example.
12. **Annexes.** Supporting documents and templates, including maps of the operating environment, contact lists, checklists and forms.

There are a number of issues to bear in mind with regard to security plans:

- Sharing plans in appropriate accessible formats and clearly explaining them to staff will help ensure their successful implementation.
- Staff who understand the reasoning behind procedures are more likely to follow them – collectively developing the plan with a diverse range of staff increases the likelihood of adherence.
- It is good practice to review plans as conditions change and events occur, regardless of when the next review is scheduled.
- Some aspects of the plan may require specialised knowledge or skills to implement.
- Effective security risk management depends on practice, through simulations and training.

Reviewing and updating security plans

Even in a stable and secure environment, security plans should be reviewed annually. In higher-risk environments, more frequent reviews are recommended to ensure that the plan reflects prevailing risks, and that the information is up to date. Example triggers for review may include:

- When there are significant changes in the external context, especially as a result of the actions of any major actors in the location.
- When there are significant changes within the organisation, such as operational approach, staff or relationships with key actors.
- When the organisation, or another organisation in or near the same operational area, experiences a security incident.

The following sections discuss two of the main elements of a security plan: standard operating procedures and contingency plans. Other sections of a security plan, such as risk assessments and crisis management, are covered in more detail in other chapters of this Good Practice Review.

▶ *For more on risk assessments see Chapter 4.1.*

▶ *For more on incident response and crisis management see Chapter 4.4.*

4.3.2 Standard operating procedures

SOPs provide detailed directions on how to carry out the specific tasks or processes needed to implement the security plan – essentially, the operating instructions for mitigating each of the assessed risks.

Good practice would call for separate SOPs, ideally written in clear and simple language, to cover all areas of daily operations where risks have been identified. SOPs can cover a wide range of activities, from daily routines to emergency response procedures, and be tailored to address the specific risks and challenges present in the operating environment. For example, in areas where road travel entails security risk, an organisation will usually establish SOPs around assessing security for planned routes, travel authorisations, vehicle safety checks, check-ins at regular intervals, speed limits and behaviour at checkpoints.

SOPs should ideally be written in clear and concise language, avoiding technical jargon, acronyms and abbreviations. Key elements of an SOP include the following:

- **Title/header** – clearly stating the name of the procedure and including document number and version.
- **Purpose** – a brief explanation of the intent and objectives of the SOP.
- **Scope** – defining what the SOP covers and to whom it applies.
- **Responsibilities** – outlining the roles and responsibilities of individuals involved in carrying out the procedure.
- **Definitions** – clarifying terms or references that may be unfamiliar.
- **Procedure** – step-by-step instructions for staff performing the task or process (the principal substance of the SOP).
- **Quality control** – specifying any quality checks or inspections required.
- **Approval/authorship signature(s)**.
- **Revision history** – a record of changes made to the SOP over time.
- **Appendices** – any supplementary materials, forms or checklists.

Having well-developed SOPs will help ensure consistency and reduce human error. When an organisation defines something as an SOP, it is typically understood to be a requirement as opposed to a guideline or advice. Because these terms are sometimes confused or used interchangeably, it is useful for the organisation to make clear to staff the level of compliance expected. At the same time, however, 'standard' means 'at most times in most cases', not that it should necessarily override professional judgement or critical thinking in exceptional circumstances. Ideally, staff will assess the situation and be able to deviate from SOPs when necessary for security or critical objectives, documenting and justifying any such departures.

▶ *For information that could be useful to guide the development of specific SOPs, see Part 7, which covers specific organisational activities and associated risks, as well as particular types of threats.*

4.3.3 Contingency and continuity plans

Contingency plans

Contingency plans support an organisation in managing anticipated high-risk events and situations where normal operations are disrupted or become untenable.

Key questions to guide the development of contingency plans include:

- What could happen?
- Who could be affected?
- What is needed to respond?
- Who needs to be informed?
- Who makes what decisions?
- What can be done to be better prepared?

Contingency plans and crisis management plans are related but distinct concepts in organisational preparedness. Crises require an organisational response beyond normal management structures. Not all contingencies qualify as crises; for example, certain disruptions, like hibernation, may be handled within normal operational frameworks without the need for crisis management. Contingency planning involves preparing for potential disruptions, and effective handling of these disruptions can require crisis management.

▶ *For more information on crisis management, see Chapter 4.4.*

In security risk management, contingency plans typically focus on situations where insecurity has risen suddenly or dramatically, necessitating decisions on whether and how to continue programming. In such cases, an organisation may be faced with the options of hibernation, relocation or evacuation (in the case of international organisations) and may approach these as progressive, escalating phases as security conditions worsen. Contingency planning may include specific triggers for each phase, or it may be a case-by-case process. Good practice would recommend setting out objective criteria to steer the decision, to circumvent the natural inclination to delay hard decisions.

Hibernation is often the first measure taken when circumstances indicate heightened insecurity. If the situation escalates, it may be advisable to relocate staff to a safer location. In extreme circumstances, international organisations may decide to withdraw some or all of their staff (usually foreign nationals) from the country, while supporting those staff members who are not evacuated. National organisations will usually be unable to evacuate their staff, and will have to rely on remote working, relocating to safer areas or suspending operations until it is safe to resume. A risk assessment should be conducted before returning to the location and resuming activities.

Hibernation

Hibernation involves stopping staff movement and programmes in a particular location by asking staff to stay at home or to shelter in an office or other organisational building. This may be because leaving the area is impossible or too dangerous, or because the situation is expected to improve in the near future. Hibernation can be a good option when staying put is safer than moving, or during temporary periods of heightened risk, such as around elections. Internet connectivity has introduced the possibility of some staff working from home, which has broadened the traditional definition of hibernation. The Covid-19 pandemic showed the viability of remote working for extended periods for staff with roles that do not require in-person presence. In Afghanistan, after the Taliban returned to power in 2021 and banned Afghan women from working for aid organisations, tacit 'work from home' arrangements allowed some organisations to continue many staff members' employment while they attempted to negotiate waivers or push back against the ban.

It is beneficial for organisations to identify a retreat or hibernation facility (and, if possible, more than one), and equip them with the following items for potential long stays:

- food, water, first aid kits and essential medicine;
- facilities for sleeping, washing and using the toilet and air circulation;
- lighting, power sources and chargers;
- fuel and equipment for cooking;
- communications equipment;
- books, games, videos or other entertainment items; and
- exercise equipment and workout and recreational space.

If bombing or shelling is a risk, organisations may need to set up safe rooms or bunkers, or identify nearby shelters.

▶ *For more details on saferooms and shelters, see Chapter 7.10 – Combat-related threats and remnants of war and Chapter 7.2 – Site security.*

Evacuation and relocation

Evacuation or relocation refer to the physical withdrawal of staff (and, where possible and provided for, their families) and assets from an insecure environment. Evacuation usually refers to movement across an international

border, while relocation refers to movement within a country. This can be precipitated by conflict or extreme hazard events, but it can also be forced, in the case of expulsion by the government. In some circumstances it may be prudent to plan a temporary, preventive withdrawal, for example removing staff from certain locations in the run-up to possibly explosive political events.

It is important to be aware of four common but often misleading assumptions regarding evacuation and relocation:

- **The deterioration will be gradual** – bear in mind that events can overtake plans. Phased planning through security levels, although useful, can create expectations of a linear progression, when this may not always be the case.
- **Evacuation and relocation will go exactly according to plan** – staff often do not refer to the plan in a sudden and acute crisis, important elements may have been overlooked and not planned for, some staff may decline to leave, and external factors may supersede earlier plans and force outcomes.
- **Leaving will be possible** – in many situations evacuation routes may blocked, the logistical capacity for evacuation may be insufficient, or it may simply be too dangerous to leave and staff will have to stay in place and weather the crisis.
- **Return will be possible** – evacuated and relocated staff may not be able to return quickly and the organisation may find itself withdrawn from the context or doing remote programme management for weeks, months or even years.

The decision to withdraw

Relocation – and especially evacuation – is a difficult decision from both a moral and operational point of view. Leaving will in almost every case mean worse outcomes for the population being served, and staying may provide a measure of protection to an endangered population, or at least a witnessing presence.

The decision may also be influenced by donor pressure or fear of defunding in the future, staff disagreements over the severity of the risk, family connections in the area, and concerns about losing acceptance and trust among the local community.

The contingency plan will need to be clear regarding who has the authority to make decisions about hibernation, relocation and evacuation, and what to do if there are divergent opinions.

Interagency considerations

In moments of serious crisis, relocations (and especially evacuations) usually require interagency collaboration. This may be complicated by differing appreciations of the risk. The fact that some organisations leave while others do not may increase the vulnerability of those remaining behind. There may no longer be a critical mass of organisations present, which may encourage looting, theft and attack. Furthermore, it is not plausible or practical for an organisation to rely on an external entity such as the UN or a foreign government for evacuation or relocation support. It is advisable for organisations to be prepared to handle these types of situation independently.

Planning for and managing the withdrawal of staff

Organisational policy regarding relocation and evacuation needs to be documented and communicated clearly to staff and partners in advance, as part of duty of care. If staff expectations differ from policy, the consequences for individual staff members, and general morale, could be devastating. As far as possible, the rights and responsibilities of employers and employees in the case of evacuations and relocations should be established in employment contracts or in the security policy, including what provisions the organisation will make for family members residing in the country. Guidance can stipulate, for example, that in times of heightened security risk, staff not engaged in programme-critical activities will be relocated or evacuated from the area.

For staff who are nationals of the country, it should be made clear what their and their dependants' entitlements are in relation to relocation (within the country) and evacuation (internationally). If discussed during the contingency planning process, these staff members can weigh their options in advance to optimise their own security and that of their dependants. It is unlikely that international organisations would be able to evacuate large numbers of national staff across international borders, but for staff members who face especially heightened risks, the organisation arguably has an ethical responsibility to help, for instance with international legal instruments and national procedures for asylum. Support for staff who remain might include providing a few months' advance salary, mobile phones, prepaid calling cards, access to the organisation's buildings for themselves and their family or letters of employment or reference.

In some circumstances, it may be appropriate for just part of a team to withdraw. Pre-emptively relocating some staff in times of rising tension, or as part of the procedure associated with a specific security phase, can lower overall vulnerability by reducing the number of people at risk, and making a potential future emergency relocation or evacuation more manageable.

Staff who might usefully be relocated in these scenarios can include any roles not vital to the continuation of the programme. Organisations can also consider withdrawing staff who face particularly high risk, regardless of whether they are in programme-critical roles. For example, certain nationalities or ethnic or religious groups may be a potential target.

An individual staff member may find it psychologically difficult to deal with rising insecurity or may perceive themselves to be at high risk. Because unmanageable levels of stress can lead to poor decision-making, it is advisable to withdraw the individual even if they are in a key operational role.

When international organisations evacuate staff who are foreign nationals and pause programming, local organisations may face increased challenges, risks and responsibilities. The following are some considerations to keep in mind.

- **Increased security risks.** Suspensions, evacuations or relocations by international organisations can change local dynamics and potentially expose local organisations to greater threats, making it advisable for those organisations to reassess their risks and mitigation strategies at these times.
- **Operational continuity.** Local organisations may need to quickly adapt to fill gaps left by departing international counterparts. This could involve taking on additional programme responsibilities or leadership roles to maintain critical services.
- **Resource constraints.** The evacuation of foreign nationals can often coincide with a reduction in funding and material support. Local organisations may need to proactively communicate with donors about continued financial needs and explore alternative funding sources.
- **Partnership opportunities.** Conversely, as international organisations may be unable to continue running programmes with limited staffing, they may turn to local organisations to continue projects. These organisations will want to weigh these new opportunities against their potential risks, such as more/different security threats and compliance demands, as well as the extra strain on staff capacity in already heightened threat environments.
- **Staff care and support**. Staff may experience increased fear, stress and anxiety following the evacuation and relocation of other organisations. Organisations can help with their staff members' wellbeing by providing psychosocial support, clear communication and flexible work arrangements where possible.

Preparing for a government expulsion – a special case

In the case of government expulsion, many of the preparations will be similar to an evacuation in response to insecurity. However, organisations may additionally want to consider the following:

- Will the organisation try to appeal against the decision and, if so, through what means (judicial, direct discussions with the authorities, advocacy or lobbying as part of a consortium, media campaigns, discussions with donors or embassies)?
- What steps have been taken to protect potentially sensitive, confidential or personal information from being inadvertently disclosed?
- Is the expulsion going to put staff remaining in the country at specific risk?
- Can steps be taken to prevent staff (especially remaining staff) from being harassed or threatened by government authorities?
- Will remaining staff be paid salaries or severance pay, and for how long? (This may be required by the government.)
- Can the risk that assets will be permanently seized be minimised?
- What role might any government donors or other actors (such as the UN) be able to play in overturning the decision or appealing to the national authorities for more lenient treatment?
- What will the media reaction be (locally and internationally) and how will it be dealt with?

Planning and carrying out an evacuation or relocation

It is good practice for organisations to regularly review evacuation and relocation plans with staff, especially if it is becoming increasingly likely that a withdrawal will be necessary. This can be done through simulation exercises or a team meeting to review policies, procedures and plans.

Logistics and route planning

When planning an evacuation or relocation route, organisations can consider the following:

- Which routes and means of transport are most feasible under different scenarios? Detailed route planning in advance, including alternative routes, is recommended.

- Which is more likely to reduce risk: moving in high profile with logos and other identifiable markings, or low profile with all of these removed?
- How much transport is available and for how many people? What kind of assets or personal effects can be taken?
- What is the most appropriate mode of transport and is it suitable for all staff? For example, staff with mobility issues may not be able to walk long distances.
- Is there safe accommodation or camping along the way if routes become insecure?
- Will communications work at all points of the route, and at which points should staff check in with colleagues?
- Who will provide transport? If not the organisation itself, it is important to understand the capacity, procedural requirements and limits of the transporting entity's responsibility and liability.
- Will the relocation or evacuation be done in collaboration with other organisations? While it can be safer to travel in a vehicle convoy with other organisations, it can also mean less control over how the departure is carried out. It can be useful for organisations to discuss beforehand how these issues will be handled.

Preparations

Plans should aim to identify sites to use as assembly points, where staff should gather before departure. Assembly points should be accessible, secure, large enough to accommodate a large number of people and several vehicles, and have reliable communications and emergency stocks.

Accurate and regularly updated information on how many staff (and dependants) qualify for international evacuation should be on hand. In general, it is helpful to have key information for all staff who may be departing, including any special requirements such as medical needs, or if any staff will be travelling with young children. Departing individuals will need to be prepared with relevant personal documentation to facilitate travel. Having essential organisational documents stored electronically (especially in the cloud) can help ensure against loss and facilitate access by staff located outside the zone of relocation/evacuation.

► *For more on protecting sensitive information, see Chapter 6.1.*

Office closure

When developing contingency plans for an office closure due to an emergency, organisations may wish to consider both asset management and

legal compliance. It is advisable to identify assets that may need securing or transferring, ensuring disposals align with donor, organisational and local government requirements. Legal obligations with landlords, suppliers and authorities should also be anticipated, to avoid delays or disputes. Security risks associated with asset transfers to partners or local communities should be assessed. Contingency plans may also include securing key assets such as vehicles and communications equipment, which might be relocated or disabled to prevent misuse. Staff may want to destroy sensitive information prior to departure.[66]

Destination

When selecting a destination for incoming staff, where this is not their home, organisations should ensure that the location provides adequate safety and comfort and access to essential services. The accommodation chosen, such as a hotel, should be secure and able to accommodate any medical, dietary or communication needs.

After the evacuation or relocation

A number of immediate, practical steps can be taken after a relocation or evacuation:

- At the first opportunity, contact the organisation's leadership to provide an update.
- If the evacuation was international, contact officials in the country of arrival (if this has not been done already), as well as relevant embassies and the local authorities if the stay is likely to be prolonged.
- Establish or re-establish contact and communications with staff left behind (see below).
- Prepare a report for head office and donors, with detailed updates on personnel, assets, stock and finance and outstanding liabilities at the point of evacuation or relocation.
- Debrief evacuated or relocated staff and provide psychosocial support, as this change may give rise to a variety of difficult feelings including emotional exhaustion and a sense of failure, anger or guilt about those left behind.

66 For more detailed guidance, see Safer Edge (2014) *Office closure*. EISF (https://gisf.ngo/resource/office-closure/).

Staff care considerations following relocation/ evacuation

Preparations ahead of arrival

- Welcome kit (including bottled water, food, toiletries, charged powerbank and charging cables, local SIM card with data plan and first aid kit).
- Identify the nearest hospital or other medical facility at the destination in case staff need medical attention upon arrival.

Upon arrival

- Provide staff with a welcome kit.
- Assist staff to contact their loved ones.
- Identify any urgent/immediate medical needs, such as any injuries or medication needing to be refilled.
- Provide staff with a security briefing about the location.
- Assist staff with obtaining local currency.
- Provide staff with contact information of the relevant support staff and their availability.
- For day one of arrival, it is recommended that the support team stay in a public/visible area (i.e. hotel lobby, café) that is easily accessible so staff can stop by for assistance.
- Staff will probably be exhausted from the journey and will want to rest in their rooms. Ask people to check in to let the support team know they are okay. For example, invite people to meet for dinner and ask them to send a text if they do not want to join, or ask people to send a text message for a quick check-in at a designated time.

During their stay

- Ensure at least one contact with affected staff per day from any member of the support team. It can be brief, such as a message or a call, or an informal social meet-up.
- Assist staff with onward travel to their homes as appropriate.
- Make sure staff know if they are eligible for meals and incidentals (per diem) during relocation/evacuation.

- Assist staff with finding local medical providers or pharmacies for prescription refills.
- Connect them with their health insurance and medical assistance provider or psychological support as needed.

▶ *See Chapter 5.4 for more on staff care.*

Continuity plans and approaches

Some organisations may not be able to relocate – this can be the case for local organisations that only operate in a single location, for example. Hibernation may take the form of closing offices and disbanding staff, 'melting back' into the community and waiting for more favourable conditions to restart programmes. Several local organisations in parts of Afghanistan used this strategy for years between 2001 and 2021, repeatedly stopping and restarting activities as political developments and security conditions dictated.

Remote programme management

When relocations or evacuations last much longer than originally planned, continuity plans may evolve into extended remote programming through partners or 'remote management' of programmes. Shifting to remote programme management can include one or more of the following:

- Withdrawing certain categories of staff (for instance, non-residents of the area in question), in particular those seen to be at especially high risk, from the programming location.
- Altering management structures to give more responsibility to staff who remain present.
- Forming new or altered operational arrangements with partners, including local organisations and authorities.
- Contracting third-party monitors to ensure programme objectives are being met in the absence of eyes-on management.

When used as a last resort and ad hoc adaptation, remote programme management usually presents serious challenges. These can include:

- Ethical problems of risk transfer, specifically if the staff members or partners taking over programme responsibilities are being asked – and strongly incentivised – to accept higher levels of risk.
- Difficulties in assessing changing security risks, and the environment generally, as staff and partners in situ may become less attuned to subtle shifts.
- Communications and logistical difficulties.
- Security implications of getting money or supplies to staff and partners.
- Over-reliance on a few staff in high-stress environments, leading to burnout.
- Difficulty in ensuring proper programme and financial oversight.
- Difficulties in meeting donor requirements for monitoring and reporting.

The practical lessons of Covid-19 have mitigated some of these difficulties, especially in terms of continuous remote communications, remote monitoring and remote training capacities – but by no means all.[67]

Security risk management during remote programming

Remote programming raises a new set of financial, security and contractual considerations, entailing a new analysis of benefits and risks. Continuing with programmes under remote management may be riskier than shutting down altogether, and there may be risks associated with closing a programme that has been managed remotely if doing so antagonises the staff affected.

If it is possible to continue operating under a remote programming approach, changes will likely be required in management structure, style and approach. Management procedures may become more complex and onerous, with frequent check-ins or reports on financial, programmatic or personnel matters. New ways of monitoring programmes may have to be developed, such as taking photos of project outputs (e.g. water sources or schools constructed), with GPS coordinates attached.

Security conditions can change rapidly, making it important to find ways to monitor the changing situation and reassess arrangements if risks for remaining staff become unacceptably high. In addition to the remaining staff, relevant information for risk assessments can be gathered through local contacts (e.g. traders and local authorities) and by sharing information and analysis with other organisations operating in the area.

67 GISF (2020) *Keeping up with COVID-19: Essential guidance for NGO security risk managers* (www.gisf.ngo/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers/).

Additional resources and training may be needed to support remaining staff or partners who have taken on additional work responsibilities, as well as funding and material support, in the form of vehicles and communications equipment, for example.

► *To learn more about partnership arrangements see Chapter 3.5.*

Other practices contributing to successful remote programme management include:[68]

- Establishing clear procedures and instructions for staff and partners on communications, and reporting on activities and progress.
- Including the remote management scenario in contingency planning exercises, considering in advance potential partners, management and monitoring structures and exit and transition strategies.
- Bringing local personnel or partner representatives out of the area for regular management meetings and discussions.
- Performing spot checks and unscheduled visits, as feasible.
- Using third-party monitors or cross-checking and verifying monitoring information with other organisations and local contacts.
- Establishing and maintaining a local network of information providers, intermediaries and facilitators within the local community.

Return

A risk assessment can indicate whether it is safe enough to return or to increase staff presence, and who in the organisation should take responsibility for the decision. In the absence of a fairly radical change at the location (e.g. a shift in territorial control from one actor to another), return may also be gradual and phased. First may come a few short exploratory missions to reassess the situation, then possibly a more permanent presence of some key staff in one operational base, followed by the gradual return of more staff and associated personnel to more operational bases.

68 Stoddard, A., Harmer, A. and Renouf, J.S. (2010) *Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas*. Humanitarian Outcomes (https://humanitarianoutcomes.org/publications/once-removed-lessons-and-challenges-remote-management-humanitarian-operations-insecure).

Case example: Return considerations

After civil war intensified in South Sudan in 2016, many aid organisations reduced their operations and evacuated foreign staff from the country. Upon re-starting its operations, one international organisation faced significant challenges implementing programmes in rural areas related to insecurity, access and communications. After several months, the security director organised a meeting bringing together representatives from various departments in the country, including programmes, finance, human resources, grants, emergency response and education.

Colleagues from the head office, regional office and national staff attended the planning meetings. During the week-long session, the team identified risks and developed mitigation strategies, created wellbeing programmes for national staff and determined the security resources required. National staff led discussions on risk and wellbeing, resulting in significant changes such as granting all national staff paid rest and recuperation (R&R) every two months.

As a result of this cross-functional contingency planning initiated by security staff, programmes resumed, donors increased their funding and the organisation's programmatic objectives were met.

Key information for assessing the security situation for an exploratory mission can include:

- The actual situation on the ground (security, military, political), as well as the personal profiles of returning staff and possible associated risks.
- Likely changes in the next 3–6 months, and their security implications.
- The status of local infrastructures (airports and roads), communications and services (e.g. banks).
- The whereabouts and status of staff who remained.

- The status of property, assets and stocks left behind.
- The availability of essential provisions, especially food, water and fuel.
- The image or reputation of the organisation locally and how perceptions can be managed.
- The level of direct targeting of aid organisations and, in the case of international organisations or those with foreign ties, foreign elements.
- Organisational capability to manage security in the current context.
- An analysis of overall risks and benefits.

Further information

Guidance and resources

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/)

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

GISF (2020) *Keeping up with COVID-19: Essential guidance for NGO security risk managers* (www.gisf.ngo/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers/).

GISF (n.d.a) *1. Security plans*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/1-security-plans/).

GISF (n.d.b) *5. Contingency plans*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/5-contingency-plans/).

Safer Edge (2014) *Office closure*. EISF (https://gisf.ngo/resource/office-closure/).

Research and discussion

Donini, A. and Maxwell, D. (2013) 'From face-to-face to face-to-screen: remote management effectiveness and accountability of humanitarian action in insecure environments' *International Review of the Red Cross* 95(890) (https://doi.org/10.1017/S1816383114000265).

Stoddard, A., Harmer, A. and Renouf, J.S. (2010) *Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas*. Humanitarian Outcomes (https://humanitarianoutcomes.org/publications/once-removed-lessons-and-challenges-remote-management-humanitarian-operations-insecure).

4.4 Incident response and crisis management

When a security incident or crisis occurs, responding effectively involves taking measures to manage and mitigate the impacts, as well as managing and learning from incident-related information. This chapter begins with the informational components before describing the key elements of response and post-incident follow-up. The chapter presents a number of structures and approaches to incident and crisis management that are generally considered good practice. However, every event and organisation will be different, and adaptation to individual circumstances, including organisational structures, is important.

4.4.1 Incident reporting and analysis

Security incident information management is the process of collecting and using information related to safety and security incidents to inform decision-making, policies and procedures within an organisation. It is an essential component of learning within an organisation and ensures that security-related experiences are recorded and analysed to improve organisational processes. This makes it an important element in meeting an organisation's duty of care. Incident reporting supports staff and operational security in four main ways: [69]

- **Incident reporting and immediate response.** To alert relevant teams so that they are aware and, if necessary, can provide help to anyone affected during an incident. Other humanitarian actors operating in the area can also be alerted in order to enhance the security of the wider community.
- **Incident analysis and lessons learned.** To analyse the incident and implement lessons to prevent similar incidents from occurring in the future, and respond more effectively if they do.
- **Context analysis.** Tracking incidents and analysing trends and patterns informs context analyses and security risk assessments. Analysing aggregated incident data from within and outside the organisation assists decision-making and indicates if procedures need to be adapted.
- **Informed strategic decision-making and policies.** To enable the sharing of security incident information internally within an organisation to inform actions and decisions to improve ways of working.

69 These points are drawn and adapted from the *Security Incident Information Management* (*SIIM*) *Handbook*, available from: https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools.

Robust security incident information management can also support organisations in meeting any legal or regulatory reporting requirements following an incident.

Incident reporting and partners

Some organisations may have partnership agreements that include the collection of incident reports from their partner organisations (though this is still rare). Partners can use this information to support each other in learning from incidents and collectively meeting any security risk management needs identified. Sharing of incident information between partners should ideally be on the basis of mutual support as a means to collaboratively improve staff security, rather than as a compliance expectation, even if for legal or regulatory reasons this may be a requirement.

▶ *See Chapter 3.5 for more good practice when working with partners.*

Incident reporting and immediate response

Organisations benefit from having well-established incident reporting procedures and ensuring that staff are trained in how to report an incident and seek help. Severe incidents should be reported immediately by the most efficient means, for example by phone or radio, and reporting should only cover the most essential information (see box below). Ongoing incidents require regular updates.

The initial report can be followed up with a debrief once staff are clear of the immediate situation and have received any acute medical and psychosocial help they need (this is different from a psychological debrief, which is discussed in more detail in Chapter 5.4). It can be useful to allow some time for those involved in an incident to talk it through ahead of gathering their thoughts for a more formal incident report. In the event of a severe incident that could affect others living or working in the area, the organisation may wish to alert people in other organisations – and where appropriate the local authorities and population – so that they can take precautions. This must be done in a way that ensures the confidentiality of those affected, and without placing staff at greater risk.

Key information when initially reporting an incident (6Ws)

- Who is involved? Who are the casualties (if any)? Are they organisational staff, partner staff or consultants? What is their gender and ethnicity?
- What happened?
- Where (as precisely as possible) did the incident occur?
- When did the incident occur?
- What has been done about the incident so far? What emergency response action has been undertaken?
- What help is needed? Is additional immediate response required? Is the situation ongoing?

It is important to alert colleagues and associates to an incident as soon as possible after it happens, when it is safe to do so, even if all information has not yet been obtained. A fuller incident report is usually written up after the incident and immediate response – although for protracted situations (e.g. a kidnapping) a report may be produced before the incident is over.

▶ *See Chapter 7.9 for more on kidnapping and abduction scenarios.*

It is good practice for organisations to have a standard incident report form that is familiar and easily available offline and online. Some organisations have invested in software that makes it possible to report using a portal or app on mobile devices. Whatever format is used, the important thing is that all the key information is provided, and it is accessible to all relevant staff. Developing simple and easy-to-use templates can encourage reporting.

The incident report can focus on some basic questions: What happened? Who did what? To whom? When? Where? (Some of this information may not be included as it is confidential.) It is important for responsible staff to verify all of this information to the extent possible. It may or may not be relevant to add something about the 'why' and 'why this organisation or staff member'. Sometimes it is obvious because the perpetrators said so, but in other instances this may just be speculation. It is important to understand if the organisation and staff member(s) were specifically targeted, and if so why, based on available

information. The report can indicate the degree of confidence in the answers to these questions, and be transparent about how much is speculation.

Under-reporting is one of the most challenging elements of managing security incident information. This can often be traced back to a lack of full understanding or familiarity with the incident reporting process, including how and by whom the information will be used. This can be addressed by having a simple reporting process, easy-to-use templates, and training staff on how and why to report.[70] Another significant challenge can be a lack of access to reporting mechanisms. This can be due to language barriers (e.g. when reporting is in English) or other factors, including organisational culture (e.g. if there is a culture of blaming or shaming, or if reporting is seen as a bureaucratic burden rather than an opportunity to learn and improve). Other common challenges with incident reports include:

- Lack of time and resourcing to report or manage incident information; in places with a high frequency of incidents it can be challenging for focal points to process large volumes of incident reports efficiently.
- Inconsistent reporting formats or procedures across different departments or offices.
- Bias and subjectivity, where reports may be influenced by personal biases, perceptions or interpretations. For example, staff may be desensitised to certain types of incidents and may not consider them relevant to report.
- Not knowing the identity of the perpetrators or their motives until much later, or in some cases never knowing at all. It is important to indicate the degree of confidence about statements, and to change internal organisational records if new details emerge.
- A natural reluctance to acknowledge that acts or omissions by the organisation or some of its personnel have contributed to an incident taking place. Staff may fear disciplinary action or other reprisals for not following organisational requirements.

70 Insecurity Insight and DisasterReady have collaborated to develop a mobile guide for staff on managing and reporting incidents. See: https://siim.insecurityinsight.org/tools-and-resources/siim-app-and-short-guides.

- Classification difficulties, for instance distinguishing between theft, burglary and armed robbery, and between abduction and kidnapping. How these different categories are defined should be clear to all reporters. Having organisational classification systems can help, and external guidance is available.[71]

It is important not to let these challenges, and confusion or disagreement over classifications and terminologies, get in the way of instituting a system for incident reporting. If staff members are not able to consistently apply classifications, if there are language barriers or if staff find the process daunting and off-putting, security staff should try to ensure that the information gets logged. Some organisations and security platforms centralise the classification of incidents, so staff can simply relay the information they have as quickly as possible, and security focal points then follow up with them to answer questions as needed and do the classification and formal entry centrally.

What counts as a 'reportable incident'?

Managerial guidance is required to ensure that people understand what they are expected to report and how – and how the information may be used. Even if in doubt, staff should be encouraged to report.

A security incident is anything that causes harm to staff or associated people, or loss of or damage to assets. A 'near-incident' or 'near-miss' is something that almost caused such harm, damage or loss. It is good practice to include incidents that have the potential to cause harm (i.e. a threat). A threatening action can be written, verbal or a physical gesture, if it credibly signifies the intent of an actor to cause harm. It is important to include even minor incidents and near-incidents.

Most organisations record both safety and security incidents, such as road traffic accidents, as well as deliberate attacks against staff.

71 See, for example, Insecurity Insight's classification of incidents: https://siim.insecurityinsight.org/tools-and-resources/classification-of-incidents.

Reporting can also include incidents or near-incidents affecting other entities involved in the programme, including partner organisations and contractors. It may also be useful to include in the reporting requirements any incident in which a staff member has caused harm to a third party, or loss or damage to the property or assets of a third party. Some other types of incidents may be included if they indicate trends in the operational environment, such as instances of community unrest or violence near project sites.

In certain circumstances, such as harassment and sexual violence, and where the incident is perpetrated by an employee (i.e. safeguarding incidents), some organisations may have separate reporting mechanisms. This can be because such incidents are usually not part of the responsibilities of the security function and also because ensuring the confidentiality and safety of the reporter is paramount. If confidentiality can be ensured, organisations benefit from also raising a security incident report. Recording incidents in one central system helps with mapping trends and putting appropriate mitigation in place.

Incident analysis and lessons learned

Follow-up with affected staff may take place at different times, depending on the severity of the incident and the way in which it was reported. It is good practice for responsible staff members, such as security focal points, to seek any additional information not covered in the incident report and organise a factual debrief with affected individuals to identify lessons. These focus on the facts of the incident rather than emotional responses to the event. When planning these meetings, consideration should be given to confidentiality concerns, whether trained professionals should be carrying out the debriefing (not necessarily security staff), and the individual needs of affected staff (such as language), and how they can be accommodated. In the event the incident occurred due to staff not following procedures, the organisation will have to weigh the need to enforce disciplinary measures with encouraging staff to report incidents.

Once information on the incident has been collected, relevant staff can analyse in more depth what happened and why. Key questions to consider during the incident analysis include the following:

- What was the cause and impact of the incident? The identity characteristics and perceptions of the organisation and individuals affected, and whether these played a role in motivating the incident, should be considered. For example, was an attack deliberately carried out against a particular staff member because of their ethnicity?
- Have similar incidents occurred in the past (including to other organisations working in the same area)?
- Were organisational procedures followed?
- Was the incident response well managed, including the reporting process? What could have been done differently?

Transparent and consistent incident reporting helps maintain trust and confidence among staff, stakeholders and the public. It demonstrates that the organisation takes safety and security seriously and is proactive in addressing concerns. Communicating with staff and others involved about lessons learned, decisions made and action taken can improve staff members' understanding of – and trust in – incident information management and can encourage reporting.

Context analysis

Incident reporting can greatly assist security staff in understanding the operational context and predicting the kind of incidents or threats that may be likely in the future. A reliable overview of reportable incidents around the world, worked through a database, allows for greater security analysis at the country, regional and global levels, as well as in relation to specific programmes and organisational or staff profiles.

Many aid organisations have internal incident reporting systems – from simple Excel spreadsheets to portals or apps displaying data visualised in dashboards.

▶ *See Chapter 3.4 for more information on dashboards.*

Having a system for managing and recording incident data standardises what types of incidents get reported, the type of information collected and how incidents are classified, allowing for greater analysis of trends and patterns. These details can reveal the geographical concentration of incidents, provide insight into incident types, and show whether the overall number of incidents is increasing or decreasing. This kind of information can in turn help in deciding where to allocate security resources (human and financial) and where more investment is needed – for example in training, technology or infrastructure

upgrades. Analysis of incident information can help ensure that resources are directed where they are most needed to enhance safety, security and operational resilience.

Analysing individual incidents and aggregate incident data is also key to organisational learning and development. This analysis helps organisations to identify trends, root causes and systemic issues that need to be addressed, and allows for targeted improvements in security protocols, training programmes and operational procedures. The information can also be used to determine and structure orientation and training for staff, visitors and travellers, as well as related protocols.

Organisations will want to manage who has access to incident databases to protect the privacy of affected individuals. However, it is important that information is shared, and organisations should allow users to view aggregated patterns and trends without revealing sensitive information about specific incidents. This can be done by putting access restrictions on databases or developing reports using data that can be shared more widely.

Comparing incident data with that of peers in the same locations can allow for a more objective incident pattern analysis and help to determine trends if the data is analysed over time. External incident data can be accessed through interagency security forums and from open-source databases (see 'Further information' below for examples). Some organisations may also have incident data-sharing agreements with each other, such as between partner organisations. All external data should be analysed considering the validity and reliability of the incident data shared. Organisations should aim to share data for security risk management in a way that ensures confidentiality and promotes collaboration.[72]

Informed strategic decision-making and policies

Security incident data can inform decision-making across an entire organisation, within and outside security functions, and organisations should have procedures for sharing and using incident data internally.

Information from incident analysis can inform programme planning, funding proposals, job descriptions and HR policies, as well as risk assessments and context analysis. Senior managers can use incident data to decide what activities and resources to finance, what security risk management measures

72 Insecurity Insight and GISF have developed guidance and tools around how to share security incident information across organisations, accessible here: https://gisf.ngo/long-read/ngo-security-collaboration-guide/ and https://siim.insecurityinsight.org/tools-and-resources/siim-in-ngo-security-collaboration.

to implement, and where and how to operate in given locations. Such analysis can also help guide strategic decisions around which contexts to work in, which security approaches to prioritise and how to communicate with different stakeholders (including donors, local groups and authorities). Incident data can also support advocacy on violence against aid workers and humanitarian access restrictions.

▶ *See Chapter 2.2 for more on advocacy.*

4.4.2 Incident response and crisis management

While all incidents require a response, the severity of the incident determines the type of response required. A non-critical incident can be dealt with using existing organisational procedures and capacity in the location where the incident took place. For this type of incident, the security focal point and other relevant staff can apply the organisation's SOPs and plans to ensure that affected staff are cared for and the broader impact of the incident is managed. What counts as a non-critical incident will vary by organisation. Examples may include low-level, non-verbal harassment, material damage to equipment, short-duration detentions, or a minor road accident resulting in no serious injuries. Non-critical incidents are usually dealt with through the management line, with additional measures possibly involving discussions with external stakeholders, information sharing with staff, and compliance with any statutory or insurance requirements (e.g. when reporting a theft). Responders should aim to always consider any personal circumstances (e.g. ethnicity, personal status or gender) that may require a customised approach.

Critical incidents are events that seriously threaten the life or health of staff. A critical incident tends to be too severe to be handled through standard management structures, requires additional support (financial, personnel, administrative and technical), and will often involve staff from multiple offices, including head office. Most critical incidents require a crisis response, meaning that an organisation's crisis management structure will need to be activated.

A crisis is a highly disruptive event that severely interrupts normal operations, causes or threatens severe consequences, and requires extraordinary measures and immediate action from senior management. Crises can take various forms, threatening an organisation's reputation, programmes, assets, finances and staff security. A crisis can be triggered by a critical incident – but not all crises are linked to a critical incident.

What is considered a crisis or critical incident varies by organisation, but common examples include a hostage situation or kidnapping, the death of a staff member, a severe attack affecting the organisation directly or indirectly (e.g. a targeted assault on staff or a bomb attack near organisational facilities, a coup or a natural hazard event, such as an earthquake).

An organisation's management response to a critical incident or crisis can be broken down into various steps.[73]

- Planning and preparedness
  - The development of a crisis management plan and structure.
  - Crisis management training and awareness raising.
- Incident and crisis management
  - The initial response, such as providing medical support and informing key stakeholders.
  - Managing the situation, such as developing and implementing a strategy to support those affected, as well as managing communications, stakeholders and information.
  - Resolution of the situation, such as the successful release of kidnapped personnel.
- Post-incident actions
  - A review of the event, the organisation's response and security risk management policies and procedures, as well as longer-term support for affected individuals.

These steps may vary in practice depending on the type of incident and its duration.

Planning and preparedness for crisis management

Effective crisis management involves having in place the right structure, comprehensive plans, training and exercises. To make decisions and take corresponding action in response to a critical incident or crisis, organisations may need to activate their crisis management plan and mobilise or constitute the crisis management structure (a framework within an organisation to deal with a crisis or critical incident).

A crisis management plan can include:

73 Henceforth described as 'crisis management', an umbrella term for both critical incidents and crises. Some organisations may use the term 'critical incident management' for critical incident response efforts.

- Definitions of types of critical incidents and crises.
- When to activate and terminate the crisis management structure, including who ultimately decides this.
- The delineation of roles and responsibilities of key actors, including the composition of the crisis management team and incident management team.[74]
- Relevant protocols and templates, such as medical evacuation protocols and incident reporting templates.

These plans can be tested regularly and incorporated into training and simulation exercises. They require review and (possibly) updating following a crisis or critical incident response.

The crisis management structure will vary by organisation and situation but may comprise the following:

- A **decision-making authority** – an individual or group with ultimate decision-making authority with regard to the crisis or critical incident – that is not normally part of the day-to-day management of the crisis, but that is regularly kept informed and, in turn, keeps other senior leadership figures and board members informed of the response team's actions. The decision-making authority is typically tasked with evaluating the severity and impact of an event or situation against predetermined criteria or thresholds that define what constitutes a critical incident or crisis requiring a crisis management response.
- A **crisis management team** at head office or the regional office, and possibly another at the country office level (for international organisations). This team is responsible for all aspects of the crisis response. Virtual crisis management teams, with staff joining from different locations, have become more common as technology becomes more reliable.
- An **incident management team** at the local level where the incident is taking place, which is responsible for implementing the incident management strategy at the direction of the crisis management team.
- **Crisis response support teams**, such as security, health, IT and communications staff, who can provide additional support without being official members of the crisis or incident management teams.

74 Henceforth, reference to crisis management teams includes any crisis management team and incident management team activated in different locations.

- Linked to the crisis and incident management teams, but often kept separate, are **family liaison support** and **crisis communications** functions. Organisations can ensure that these form part of their preparedness plans (see later sections).

The crisis management team can establish hierarchical responsibilities and draw a clear distinction between the roles played at the different office locations (e.g. project, regional or head office). A clear organigram can be developed and kept up to date, with defined responsibilities and a contact list. Everyone involved should understand where they fit in. For some incidents an incident management team may operate only at the local level, but there needs to be a clear understanding of when to involve head office (including regional crisis response teams where applicable). Serious or prolonged incidents (an assassination, bomb attack, kidnapping or forced hibernation, for example) or major changes (such as a relocation or evacuation) will typically require a dedicated crisis management team, supported by an incident management team. The exact distribution of responsibilities across these teams will depend on the context and situation. For example, designating trained family liaison officers to support affected staff and their families can be done at both the crisis and incident management team levels, depending on the situation.

Ideally, crisis management teams should be small for agility and speed in decision-making. They can include representatives of a number of core functions (see the box below). A crisis manager may be appointed with the authority to commit the appropriate personnel, equipment, finances and other resources to ensure an effective and timely response. Information management should be considered carefully within the crisis management team and supporting functions, particularly as those individuals who are tasked with engaging with external stakeholders (such as family liaison and communications staff) may be placed in an uncomfortable position if they are privy to all information.

Crisis management is challenging and requires a range of competencies and expertise – legal, medical, psychological and hostage negotiation, for example – some of which may need to be found outside the organisation. Any requirement for external support should ideally be identified and that support obtained early, and used for as long as is required (which can vary from an initial consultation to more regular input during the response period). Some organisations draw on former staff members who know the organisation and whose competencies and experience are recognised and trusted. Existing staff members external to the crisis and incident management teams with relevant knowledge, contacts and skills may also be involved.

Crisis management team functions

The composition of crisis and incident management teams will vary depending on the organisation and the event being responded to. Some functions that organisations might want to consider include:

- Team leader/crisis manager
- Human resources
  - Administrative support (e.g. personnel files and insurance liaison)
  - Family support (coordination of family contact and support, management of family liaison officers)
  - Staff support (psychosocial care for affected staff, including responders)
- Media and communications (usually implemented by a separate crisis communications team)
- Assistant to support with administrative tasks, including taking notes and arranging meetings
- Depending on the nature of the incident or event, security focal point, country director, head of operations in the location, experts in the context, medical, legal, logistics and IT.

Not all individuals responding to a critical incident or crisis will necessarily be based in the same location. Crisis management can involve remote and virtual collaboration and coordination between team members.

Crisis management can initially be a full-time job. Staff involved need to be released from their other duties and shielded from unnecessary intrusions so that they can concentrate on the task at hand. They benefit from having their own working space and facilities, including a temporary crisis room. They should aim to monitor the situation on a daily basis, and regularly decide on and review policy towards different stakeholders. Team members may need regular rest and relaxation as well as support during and after the crisis.

Personal information file

Human resources staff can support crisis management by ensuring they have appropriate information and documentation on hand for all employees in the event of a crisis or critical incident. Some organisations maintain a personal information file with key information such as:

- Proof of life information
- Emergency contact(s) (which may be different for different circumstances)
- Medical information
- Social media information
- Additional details that may be relevant when liaising with family or providing emergency support to the staff member.

This file will need to be handled with the utmost confidentiality, but should be quickly accessible in an emergency.

If the crisis continues over an extended period, members of the crisis and incident management teams may have to be rotated. Leave plans, travel and other work commitments can also affect how long individuals can fulfil their crisis management functions. A smooth changeover can be prepared for by making sure that a handover file is kept updated with reports and analysis, and that the handover is planned so that team members overlap. Good practice suggests having one or two backup staff for each role – all trained and prepared to step in should it become necessary.

Crisis management training is one of the most important components of preparing for a crisis or critical incident. All staff identified for a crisis or incident management role need to be trained and feel comfortable working together. Funding is needed for preparedness training, including simulation exercises.

Crisis management training

Crisis management training and exercises can take different forms – from tabletop exercises to full-scale simulations. Initial discussion-based exercises identify key responders, capabilities and gaps. More advanced simulation exercises test crisis plans in realistic scenarios. Regular training and exercises in crisis response and communication improve decision-making, awareness and confidence in an organisation's ability to effectively manage crises and critical incidents.

Initial response and strategy

The first step in dealing with a critical incident or crisis is to decide whether immediate action is required to preserve life or ensure safety. Verifiable information must be established outlining the details of the event. This can be part of the initial reporting. Additional information or changes should be advised as they occur.

A log should ideally be initiated immediately after an incident is reported and regularly maintained to record the chronology of events, log phone calls, record notes of meetings and ensure that all documents are recorded and filed.

On receiving an incident report, the first decision is whether a particular situation qualifies as a crisis or critical incident, and whether to activate the organisation's crisis management structure. As it is often easier to stand down a crisis management response than to scramble to catch up, organisations may consider operating on the basis of 'prudent overreaction'. If the crisis management function is activated, the team may have to decide:

- Whether programme activities should be suspended, or personnel withdrawn to a more secure location.
- If additional support personnel should be deployed to assist.
- What information should be circulated internally and externally, and any limitations or confidentiality issues.
- The end-state objective (e.g. injured person evacuated, body repatriated, kidnapped staff member released).

The importance of keeping a logbook

An important element of incident and crisis management is the opening and maintenance of a logbook to record decisions made, the reasons for these decisions, who made them, when and any resulting actions. The benefits of doing so include:

- It provides a full record to facilitate handover to new crisis management team members in a prolonged response.
- It can help inform post-incident/crisis actions.
- It provides documentary proof that the organisation has done its best to fulfil its duty of care to affected staff.
- Records can demonstrate that the organisation used a considered and systematic approach to decide what actions to follow, even if these did not have the intended results.

It is advisable for the information in the logbook to be carefully managed and kept securely, with confidentiality maintained and respected.

A key role of the crisis management team is to develop a crisis or incident management strategy, which informs the organisation's approach to the event, including:

- Stakeholder management, including family support and liaising with authorities, media, communities and other organisations.
- Communications.
- Negotiations and communicating with the perpetrators, if applicable.
- Information management, including information gathering and analysis, maintaining information security, record-keeping and documentation.
- Resourcing (material and human).

The strategy should be informed by relevant experts, such as legal counsel to ensure that it considers applicable legal frameworks and jurisdictions. Each incident should have its own strategy, which should be reviewed regularly.

Overall, the crisis management team usually has to consider medical and security issues, logistical support and surge capacity and reputational, legal, communications and media issues. The crisis management team may need to liaise with insurance providers and ensure adequate coverage, disbursements and support. There may be injured people who require immediate or long-term care. If lives are lost, family members will need to be informed and measures taken to provide for funeral, burial and other expenses. Security may still be a concern if individuals not caught up in the actual incident are still at risk and logistical support may be needed to organise medical evacuations, repatriation or the return of bodies to their families. Depending on the situation, specialised staff may be dispatched to the affected location, for instance to provide search and rescue capacity, medical or forensic help and psychological and counselling support. Other offices, at regional and/or head office level, may also require such expertise.

The incident management team plays a key role in implementing the directives of the crisis management team, which can include responsibility for:

- Management of the crisis at the local level.
- Communication with local stakeholders, including family, local authorities (including police), embassies and other government representatives, UN and NGOs and local media.
- Providing support for the family, if present in the location, and moral and material support for affected individuals, if possible.
- Information sharing and assessment of risks for the crisis management team at head office.

Communication and media management

Communications management is a crucial component of managing a crisis or critical incident. Given the risks associated with leaked information, confidentiality and adopting a 'need-to-know' approach are considered good practice. The GISF *Managing the message* guide shares detailed guidance and tools on how to manage communications with internal and external stakeholders during a crisis or critical incident.[75]

75 Davidson, S. (2013) *Managing the message: communication and media management in a security crisis.* EISF (www.gisf.ngo/resource/managing-the-message/).

Coordination in times of crisis or critical incidents

Some events may require coordination between multiple organisations, such as an attack on a convoy or a group kidnapping. In these circumstances, the organisation's crisis management team would be liaising with key stakeholders, and potentially sharing information, advice, contextual expertise and resources with other organisations.

Where multiple organisations decide to relocate or evacuate staff in the event of a major crisis, such as civil conflict, organisations may rely heavily on the same resources or the UN for support. Coordination in these circumstances is key but can be challenging in practice, as resources may be overwhelmed and access limited. It is essential for all organisations to be clear on what support they require during these types of events, and confirm these are in place before an event occurs.

It is always good practice to establish relationships with outside stakeholders before an event occurs, and for all actors to be clear on what support they can expect from each other and what the coordination mechanisms are. A good starting point is for organisations to establish contact with relevant actors, including other aid organisations and the UN, on entering a new area and asking what coordination in the event of a major crisis would look like.

▶ *See Chapter 2.1 for more details on coordination mechanisms between organisations.*

Communication and media crisis management plans form an important part of crisis management preparedness and should be in place prior to a critical incident or crisis. While communications with internal and external stakeholders should be directed by the crisis management team with support from a crisis communications team, the latter is primarily responsible for dealing with the media, developing and implementing the communications and media strategy,

prepping and drafting communications for external and internal audiences, monitoring the media (including social media) and designating a spokesperson.

The crisis communications team might include an overall team manager, a spokesperson, a media monitor and support staff. As with the crisis management team, it is good practice for this team to be properly trained and to regularly practice implementing the organisation's crisis communication and media plan.

The crisis communications team takes on responsibility for communications-related activities, often at the direction, in conjunction with or with final approval from the crisis management team, such as drafting key messaging for different groups (internal and external) and agreeing on a media strategy.

Communications at the project and country level

Many people and organisations may have to be informed rapidly at a time of crisis. Rather than have one person try to do this, organisations can establish a communications tree or network in which each 'node' has responsibility for passing on information to three or four other nodes. An easy way to do this is to use the staff organigram. This can be updated regularly at preset intervals so that names and contact information are accurate and maintained/updated immediately if there are staff changes. It can also be clarified in advance whether phone calls, SMS or radio will be used. A warden system, if in place, can be integrated into this. In times of emergency, national communications networks are prone to failure or overload: if possible, the organisation should ensure alternative means of communication independent of the national infrastructure.

If the incident calls into question the continuation of programme activities or even the organisation's continued presence in the location, it may be necessary to communicate with affected communities, key stakeholders (e.g. authorities), the general public and key donors.

Communication between organisational teams and offices

Reliable, dedicated, well-resourced, round-the-clock and secure communications is often needed between the location affected and the different crisis management teams. It is advisable to anticipate a temporary loss of communications and prepare accordingly. Translation support may be needed if there are language differences between stakeholders and teams. Rumour control within the organisation is important, as speculation will likely be rife and expressed in multiple ways, such as through social media, messaging apps and email. Effective internal communication with other organisational staff should

be proactive and well managed. It is advisable for organisations to anticipate questions and maintain staff morale and confidence in the organisation, while at the same time trying to keep non-core staff at arm's length from the crisis management effort.

Communication might involve:

- Regular or as needed information sessions for all staff, given by the head of the crisis management team.
- An information sheet accessible to all staff (in multiple languages if necessary) and posted on the intranet or through another communications medium.
- Providing staff with opportunities to feel engaged and to show their support for affected colleagues, for instance by signing messages of support – affected staff seem to appreciate such efforts once incidents have been resolved.

For a serious incident or crisis, the organisation's board members may need to be kept informed and consulted on critical decisions.

Communication with the media

Severe incidents affecting a staff member (such as death or injury) will usually necessitate immediate notification to the family, usually followed by a statement or press release from senior staff. Sometimes the notification is made by other entities, such as the embassy or local authorities, and in these circumstances the organisation should try to follow up with the family as soon as possible. A press conference may also be called, or a press release issued.

Organisations should have a prepared media plan that can inform the media strategy adopted for a particular crisis or critical incident. Organisations can identify individuals ahead of time to speak to the media – this may be a designated spokesperson – and offer training to these staff. The spokesperson is closely linked to the crisis management team, though usually not a formal part of it. It is advisable that these individuals are nonetheless involved in crisis management team training.

It may be necessary to communicate with the local, national and international media – and to be prepared when they contact the organisation. It is important for organisations to be aware of discussions taking place about incidents and the affected staff on social media. Social media influencers may make content about high-profile cases, and the organisation's media team may need to monitor these

platforms and be prepared to respond if necessary. Organisations that do not have media professionals on their staff can seek professional advice externally.

In certain circumstances, it may be appropriate to post a statement on the organisation's website, intranet and relevant social media platforms. Given the proliferation of information, note that any statement made publicly can have global reach. Communications shared with staff may be leaked to the media. As a general rule, the identities of affected staff should always be kept confidential. Within the organisation, it should be clear what information is to remain confidential, who is included in the information circle and how confidentiality will be protected.

Social media considerations

Communication shared via social media platforms can trigger highly negative sentiments in the aftermath of an incident. For example, following a deadly attack on two international NGO employees in Burkina Faso in 2023, an analysis of social media reactions revealed widespread misunderstanding and negativity towards the organisation and humanitarian work more generally. Several commentators accused the organisation of collaborating with armed groups and serving as a proxy for western governments. The organisation's publicly stated intention (on the day of the incident) to initiate dialogue with all the parties to the conflict resulted in significant backlash on social media platforms, with many comments interpreting it as an attempt to legitimise Islamist armed groups.

Social media monitoring to gauge local sentiment towards aid organisations is an increasingly important aspect of measuring local perceptions, acceptance of aid work in operational contexts and security risk management. This type of monitoring becomes more important still during crises and critical incidents. Some organisations are investing in this monitoring work directly, while others rely on public sources (for example, Insecurity Insight's social media monitoring reports: https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring).

Source: Insecurity Insight (2023) 'MSF ambush in Burkina Faso' (https://insecurityinsight.org/wp-content/uploads/2023/03/MSF-attack-Burkina-Faso-Social-Media-Monitoring-March-2023.pdf).

The main objective of all media activities should be to protect affected staff; in some critical incident cases this can mean keeping a low profile, but in others it may mean raising media profiles in a carefully managed way. In some critical incident cases, such as abductions, the perpetrator's main purpose may be media attention. In some contexts, media are not allowed to publish details about sexual violence cases, and even where this is not banned, if the identities of survivors are leaked, they risk facing stigmatisation or further victimisation.

Communications with neighbours and other organisations

If the organisation's office has come under attack, for example, it is advisable to speak to neighbours, whose sense of insecurity has probably been heightened. It may also be necessary to alert other aid organisations about a major security incident, so that they can take precautionary measures.

Family liaison and support

Supporting and liaising with the family of affected staff members is a critical part of managing an incident. At its core this involves ensuring that the family feel confident that the situation affecting their loved one is being handled well by the organisation. Not only is this an important aspect of duty of care: failure to do so could also undermine the organisation's crisis management efforts. Family members who do not feel confident in the organisation's response may, for example, go to the media, or arrive in the crisis area with their own plans. While these actions are in themselves not problematic (it may sometimes be advisable for family members to make statements or for the organisation to facilitate their presence in the location), uncoordinated actions can interfere with the organisation's crisis management plan. In 2017, EISF (now GISF) developed *Family First*, a detailed guide on family liaison and support during critical incidents and crises.[76] The following section covers some basic considerations.

In the first instance, an organisation should communicate with the families of staff and others affected by an incident. Every effort should be made to ensure that the family members of affected staff are the first to be informed about an incident. It is good practice not to issue any messages or statements until family members have been informed directly by the organisation's staff.

The crisis communications team can work alongside family liaison staff to support family members who may suffer from media intrusion, which may include shutting down social media accounts of the affected staff and family

76 Davidson, S. (2013) *Family first: liaison and support during crisis*. EISF (www.gisf.ngo/resource/family-first/).

members. This action can also block hostile groups, including perpetrators, from accessing personal information and using it maliciously. For this, organisations should ideally have plans and, where possible, established routes of communication with social media and other platforms to close accounts or take down articles that may compromise the safety and privacy of affected staff or family members.

Support to families may also require a more active engagement depending on the nature and length of the incident. It is also important for organisations to be aware that families may take initiatives themselves, especially if the incident lasts for a long time. It is important that they feel empowered to do so, but that their plans and actions coordinate with the organisation's crisis management plan as much as possible. To support family members of affected staff, organisations should consider:

- Identifying the emergency contact, and taking note of any personal circumstances that should guide interaction with the family.
- Selecting the news bearer and the family liaison focal point. Usually, the individual making first contact with the family member will be a more senior staff member within the organisation, and support can later be provided by the family liaison focal point.
- Breaking the news without delay with frankness and compassion.
- Introducing the individual designated as the focal point for the family members, and explaining their role and how to contact them.
- Assessing and meeting the family's immediate needs.
- Ensuring confidentiality and establishing two-way trust between the family and the organisation.
- Setting up a regular contact schedule with the family.
- Managing information flow between the organisation, the crisis management teams and the family.
- Bringing in external services and advisors to support the family.
- Maintaining written records of communication had and decisions made.
- Developing an exit strategy – for example, following resolution of the incident or if the incident is never resolved.

A trained staff member with good interpersonal skills can be designated as the focal point for the family. The individual selected should be able to converse

with the family in their language and be trusted and accepted by the family. Some organisations have a family liaison post (sometimes called a family liaison officer) expressly for circumstances such as these, while at other times it may be an individual already known to the family, such as the affected staff member's supervisor who is in turn supported by a trained family liaison function. Where organisations do not have a specific post for this, it is good practice to have at least one or two existing staff members trained in family liaison who can take up this role in the event of an incident. One function of this post is to act as the designated contact person for the family (where several individuals have been abducted, it may be necessary to identify several individuals to act as interlocutors with affected families). The same individual should ideally play this role throughout the incident, although in practice this may be challenging for long-duration incidents. This is a demanding responsibility and will often require support from the organisation.

The family liaison post is usually not a formal member of a crisis management team, although they should be aware of the team structure and ways of working, and keep in regular contact. However, they should not be involved in the day-to-day operational management of the incident or crisis, which allows them to focus on supporting the family fully. The tasks of a family liaison focal point can include:

- Acting as the sole channel of communication between the organisation and the family.
- Establishing and maintaining regular contact with the family, including being on call at all times in the case of an abduction or kidnapping.
- Guiding the family on what to do if they are approached by the media or perpetrators (e.g. kidnappers).
- Sharing information, guidance and support from other teams, such as the crisis communications team.
- Arranging salary payments and other support to the family.
- Liaising with others as appropriate.

Personal circumstances may require additional tact and sensitivity when liaising with family members. Family units can take various forms and structures. In certain situations, a family may be divided or separated. Additionally, there are cases where a staff member's romantic partner may not be known or acknowledged by their relatives. Family relationships and dynamics can be complex and non-traditional, deviating from conventional norms. It is imperative that family liaison staff consider the wishes and needs of affected staff. Some

staff members, for example, may not wish their families to know about particular incidents, such as sexual violence. Other staff may wish personal information to be kept confidential from their families, such as their sexual orientation or medical history. Organisations should have named emergency contact information in staff personnel files, which may list special circumstances that can be incorporated into family liaison work, including different emergency contacts for different types of situations.

Relations with the authorities

Organisations may need to coordinate with authorities including the government of the country where the incident or crisis has taken place and, if different, the government of the country of origin of affected staff members. It is also not unusual for aid workers to be nationals of different countries, meaning that there may be several 'home countries' to consider. A range of different government departments and institutions may also become involved.

Agreement and collaboration with authorities may be needed for the rapid processing of visa applications for crisis support or other surge staff. Governments may mobilise their own experts depending on the type of incident and the nationalities of those affected. This can create a difficult situation in terms of responsibility and duty of care. If another entity takes the lead, organisations can argue for what they consider to be in the best interest of the individuals affected – hopefully in alignment with the family's wishes. It may be possible to pre-empt this by asking relevant government officials what actions they would expect to take in the event of a particular incident.

Administrative, legal and financial considerations

Some situations may require legal advice. This advice may pertain to terms of contracts, employee benefits, insurance questions, legal rights under applicable labour laws, legal representation with a host or home government, or dealing with legal challenges and claims for damages.

Managing a critical incident or crisis, particularly a prolonged one, also requires administrative support and specialised human resources. There may be other urgent expenses for travel, equipment or external services. Affected staff may be temporarily unable to work because of physical injury or psychological stress, and it may be necessary to bring in temporary replacements and provide wellbeing support. Organisations may require extra cash because of unplanned and non-budgeted expenditure, including as part of the implementation of the crisis response strategy. Some of this expenditure may be covered by the organisation's insurance.

► *To learn more about insurance and staff care see Chapter 5.4.*

Post-incident management

Deactivating the crisis management response

There will come a point when the crisis management structure stands down, often when an incident is considered 'resolved', for example when the individuals affected by an event are no longer in danger and have received necessary support. It may be that there is no clear resolution, however, such as in the case of missing or abducted staff. These types of incidents can last many years, and an organisation may decide to stand down the crisis response even in the absence of a resolution. Organisations should have a clear process for deciding when and how to deactivate and disband crisis management teams.

Post-incident staff care

Care for affected individuals may need to outlive the organisation's crisis response. Organisations may need to be prepared to provide long-term support to staff and others affected by an event.

Following an event, affected staff may require support in a number of ways, including:

- Reception upon release into the organisation's care (in the case of detention, arrest or abduction).
- Immediate medical and psychological attention.
- Immediate material support, such as accommodation and other materials for their comfort and wellbeing.
- Relocation or evacuation support.
- Support to reunite with family.
- Communications management following the incident resolution, in line with the affected staff member's wishes, which can include guidance on how to deal with media requests.
- Return to work plan.
- Guidance on accessing support services, including insurance and long-term medical and psychosocial care.
- Guidance on how to seek justice against perpetrators.

Individuals involved in the management of the incident or otherwise affected by it (such as team members of the affected staff member), including family, may also require support following a severe incident.

A survivor-centred approach will help ensure the affected staff member feels empowered to make their own decisions regarding their recovery, while being careful not to overwhelm them with too much information or too many choices, and working alongside their wishes and within their capabilities (which can change over time).

► *To learn more about the survivor-centred approach, post-incident staff care and insurance, see Chapter 5.4 on staff care.*

Debriefing and after-action review

Everyone who was directly involved in the management of the incident or crisis should have the opportunity for a factual debriefing. This may also include individuals who were close to the situation but not directly involved in its management. Any crisis, incident or near-incident affecting the organisation, its programmes, its partners or its contractors merits analysis, and an after-action review (sometimes called a post-incident review) is widely considered good practice. For serious events, organisations may consider a more thorough and, ideally, independent evaluation of why the situation occurred, how it was managed, and why it had the impact it did. Following any serious security event, a review of existing security and safety policies and procedures is warranted.

Key questions to consider include the following:

- Were security measures in place and understood by staff?
- Were security measures followed?
- Were security measures appropriate to the threat?
- Were warning signs of a specific impending threat observed, and if so, were they acted upon in advance of the event?
- Conversely, were there no warning signs, so the event was not foreseeable?
- Was the risk of a specific threat occurring accurately assessed, and appropriate security measures put in place, but the event occurred anyway?
- Were crisis management teams both pre-identified and -prepared?

Essentially, organisations should aim to assess whether there were weaknesses or compliance issues relating to the risk analysis and risk mitigation strategies employed. A review of the crisis response mechanism is also good practice in order for the organisation to make any necessary adjustments in preparation for any future critical incidents or crises.

It is important that debriefings and after-action reviews are conducted sensitively and are survivor-centric. This involves considering what information may be disclosed in these sessions, including physical and sexual violence for example, and how this should be managed and reported.

Any serious incident affecting another organisation operating in the same environment also merits attention and analysis. That analysis may not necessarily conclude that the organisation is at heightened risk. There may be various reasons why what happened to one organisation is unlikely to happen to another. The ability to conduct a reasonable analysis of an incident affecting another organisation may depend on how much reliable information can be obtained.

It is imperative that, if the post-crisis analysis indicates follow-up actions (such as additional training or amendments to risk analysis and security procedures), an action plan is developed and an implementation mechanism (with clear responsibilities) put in place to ensure changes are made. In many cases, the action plan is not adequately implemented after a crisis management team disbands and its members return to their normal work. The findings of the after-action review should ideally be shared with staff, possibly with different levels of detail depending on the level of involvement in the incident. Information may be presented to other organisations if it concerns them, and this information needs to be shared in a way that does not compromise the affected staff member.

Review the threshold of acceptable risk

Any serious security event, whether it affects an organisation directly or not, should usually trigger a review of the organisation's threshold of acceptable risk. If the incident involved partners, an organisation can consider whether their risk exposure is acceptable. Does this event signal that the initial analysis was flawed? Does it indicate that the organisation has crossed the threshold of acceptable risk? What are the practical consequences? Can security measures be strengthened to reduce the risk? Should there be changes to the operational security strategy, and will these changes be effective? Should staff be relocated away from areas of high risk? If adjustments or changes are required, staff should be assigned to ensure that these changes are implemented, and a timeframe established. This may require new or additional training.

This is an appropriate point to share with all staff the new assessment of the security situation and of the nature and level of risk, as well as the likely effectiveness of the organisation's security measures. It also presents an opportunity for staff to be informed of any changes in the situation/context and revisit their individual risk thresholds.

Further information

Guidance and resources

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/).

Buth, P. (2010) *Crisis management of critical incidents*. EISF (https://gisfprod.wpengine.com/resource/crisis-management-of-critical-incidents/).

Davidson, S. (2013a) *Family first: liaison and support during crisis*. EISF (www.gisf.ngo/resource/family-first/).

Davidson, S. (2013b) *Managing the message: communication and media management in a security crisis*. EISF (www.gisf.ngo/resource/managing-the-message/).

EISF (2017) *Abduction and kidnap risk management* (www.gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

GISF (2021) *GISF – Remote crisis management course* (www.gisf.ngo/resource/gisf-remote-field-crisis-management-course/).

GISF (2022) *NGO security collaboration guide* (https://gisf.ngo/long-read/ngo-security-collaboration-guide/).

GISF and Overseas Security Advisory Council (OSAC) (2023) *NGO crisis management exercise manual: a guide to developing and facilitating effective exercises* (https://gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/).

Insecurity Insight (n.d.a) *Security incident information management (SIIM)*. (https://siim.insecurityinsight.org/).

RedR UK, Insecurity Insight and EISF (2017) *The security incident information management handbook* (https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools).

Open-source security incident databases

Humanitarian Outcomes (n.d.) *Aid Worker Security Database* (www.aidworkersecurity.org/).

Insecurity Insight (n.d.b) *Aid in danger* (https://insecurityinsight.org/projects/aid-in-danger).

Insecurity Insight (n.d.c) *Social media monitoring* (https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring).

INSO (n.d.) *Humanitarian Data Dashboard* (https://ngosafety.org/ngo-data-dashboard/).

5 People in security risk management

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/).

5.2 Security training

Security training within the humanitarian sector has grown significantly in recent years and, although it has drawn learning from the private and government sectors, it has evolved into a unique and diverse area of practice. Despite much research, general guidance development and efforts to improve the quality and consistency of security training in the sector,[80] there is still no standard approach to security training.

The following chapter covers existing approaches to security training, including the benefits and challenges of different types of training, and key considerations for organisations regarding basic needs and equity of access to these resources.

5.2.1 Why is security training important?

While this GPR focuses on the work of security staff, many, if not most, security decisions are made by individual staff members. For that reason, all staff, no matter their role, should be able to make informed security decisions to avoid incidents and respond effectively in the face of threats. Security training plays a foundational role in this and is a key building block in meeting duty of care obligations and creating a positive security culture.

5.2.2 Types of security training

Security training can be divided into three categories:

- General safety and security awareness, provided to staff through inductions and briefings.
- Personal safety and security skills training, such as hostile environment awareness training (HEAT).
- Security risk management training for staff with security responsibilities, which can include crisis management training.

A potential fourth category is strategic security risk management training for organisational leaders – usually senior management and security directors. This covers issues such as how security interfaces with other organisational

80 Such as the NGO Safety and Security Training Project by EISF and InterAction (2014): https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos

processes and risk management, as well as how it fits into other policies and areas of work, especially duty of care. This level of training is rare.

Security awareness: inductions and briefings

Basic safety and security awareness training is commonly provided to staff at the beginning of their employment with an organisation or when they arrive in a new location. These sessions are generally brief and focus on providing staff with a general overview of the organisation's security policies and procedures, including resources and contact points, as well as key roles and responsibilities (including staff members' own responsibilities). In this sense, awareness sessions are different from most personal safety and security training, which tends to be more generic and does not always cover organisational procedures.

Security awareness sessions can focus on particular types of risks – often related to a particular context – and may also cover broader challenges, such as issues relating to identity-based risks and other concerns e.g. digital threats. Sessions may also cover safety risks, such as fire safety, especially in project locations, though these may occasionally be covered separately from security discussions, especially where organisational focal points for security and health and safety are separate. These types of awareness-raising sessions can become tick-box exercises, especially if they are provided online and do not offer opportunities for questions.

Table 7 Security awareness briefings: example content

Example content	Description
Security approach	An explanation of the organisation's approach to security, its duty of care obligations to staff, the risks its staff face and the organisation's attitude to risk (i.e. risk appetite).
Security policy	An introduction to the organisation's security policy and other relevant policies, including related key principles and security requirements and their application.
Security risk management structure	An overview of the roles and responsibilities with regard to managing security within the organisation.

Example content	Description
Expectations	The organisation's expectations of individual staff, including their responsibility for their own security and that of their colleagues, and relevant actions and behaviours. It can also cover what staff should expect from the organisation regarding security, including the right to withdraw or say 'no' if they feel a situation is insecure.
Travel security	The organisation's security arrangements for travel.
Emergency procedures	An explanation of the organisation's procedures in the event of an emergency, such as medical assistance. This can include providing staff with all necessary information for them to report an incident and seek assistance (e.g. how to call the medical insurance provider).
Incident reporting	An explanation of what incidents should be reported and how to report them.
Resources	Staff are provided with relevant resources, including documents, online resources, handbooks, guides and training material.

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/).

Personal safety and security training

More in-depth personal safety and security training may be appropriate for staff working in higher- risk locations. These courses tend to be longer – some lasting several days – and can be provided by qualified staff within an organisation or external service providers.

While security awareness sessions tend to focus on building an understanding of – and adherence to – organisational security protocols, personal security training is often more generic and usually focuses on developing behaviours and skills to keep staff and their colleagues safe. Table 8 below lists some example learning objectives.[81]

81 For more learning objectives in personal security, see EISF and InterAction (2014).

Table 8 Example learning objectives

Objective	Description
Situational awareness	Consideration of surroundings and local perceptions.
Security conscious	Awareness of – and personal responsibility for – decisions and actions that can affect personal and organisational security.
Personal risk profile	Awareness of how each member of staff may be perceived through their appearance or actions, including any displays of wealth or status, confident and composed behaviour, tactful and diplomatic language, and respectful attitudes towards local cultures and customs. It is also important to be clear that sometimes personal profiles are misperceived or cannot be mitigated at an individual level (such as where there may be ethnic targeting or negative attitudes towards women).
Communication	Remaining in contact with colleagues as appropriate and in line with organisational expectations.
Personal response	Empowering staff on how to respond effectively to threats, hostility, crises and stress.

The level of detail and duration of a personal security training course is generally determined by the level of risk a staff member may face. Personal safety and security training can take many forms, but ideally should be adapted to each organisation, the needs of staff and the location in question. What works for one organisation or location may not be suitable for another. Security training courses have become increasingly professional and widespread in recent years (though with varying levels of quality and credibility), with many considering hostile environment awareness training (HEAT) the 'gold standard' in personal security training for high-risk contexts.[82] While there is no set format for HEAT courses, they typically last 3–5 days and involve a combination of classroom-based learning and exercises and more in-depth simulation scenarios, which generally involve placing participants in life-like stressful situations with props and actors.

82 HEAT is the predominant type of training, although there are a number of variations, including hostile environment and first aid training (HEFAT) and hostile environment training (HET).

Many argue that the simulation component makes HEAT different from general personal safety and security courses. Quality HEAT courses are based on the principles of high-fidelity stress exposure training (or stress inoculation training), developed in the field of psychology. Research on high-fidelity stress exposure training in professions such as medicine and aviation supports the effectiveness of such training when it:

- conveys knowledge and familiarity with the stress environment to form accurate expectations;
- conveys knowledge about the effects of stress on the brain and behaviour and how to control these responses safely; and
- builds confidence in the person's ability to perform in gradually more stressful scenarios.

HEAT simulations allow individuals to witness their instinctive reactions in highly stressful situations. Whether they tend towards 'fight', 'flight', 'freeze' or 'friend/fawn' (i.e. capitulate and comply) responses, they will be more equipped to manage these reactions in real-world scenarios. By practising skills under pressure and stress, the hope is that trainees will better retain and apply the knowledge should it be needed.

Some HEAT courses also cover trauma first aid. Most HEAT courses are provided by specialised external service providers. In some contexts, country-level entities offer open HEAT courses.

In addition to general personal security training courses and HEAT, there are other courses relating to personal security – the UN, for example, has developed security training specifically for women called the Women's Security Awareness Training (WSAT).

Since the Covid-19 pandemic, more personal safety and security courses are being provided online and in modular format (both facilitated and non-facilitated), with some providers also advertising online HEAT courses. Free online personal security courses are also increasingly available on training platforms targeted at humanitarian workers.[83] Some larger organisations have developed in-house online security training.

83 Examples are in the 'Further information' section at the end of this chapter.

Some organisations and training providers have opted for a blended approach to training, where a portion of the training is provided online, followed by an in-person component with exercises and simulations.

Simulation-based security training: potential downsides

HEAT courses are an area of contention within the humanitarian security community. While often described and seen as 'the' security training for working in high-risk locations, with some staff expecting it from their employing organisations as a matter of course, its limited availability and accessibility and high cost make it a commodity available to only a select few aid workers (although the expansion of the sector has increased its availability in recent years). While to date, there have only been a few studies demonstrating the effectiveness of HEAT simulations,[i] research on how the brain responds to threatening situations indicates that previously learned cognitive information becomes unavailable unless it is also solidified with more visceral experiences.[ii]

The quality of the simulation of a HEAT course can vary from well-managed, psychologist-supported and moderately stress-inducing simulations to more extreme simulations that can be physically and psychologically distressing. Training courses intend to promote skills retention but, if pushed too far, especially without psychological support, the stress experienced by trainees could have the opposite effect. More concerning is the risk of traumatisation or re-traumatisation in security training simulations, depending on how sensitive a participant may be to certain triggers.

While the most extreme simulations – hostage-taking scenarios, for example – are now less common in the humanitarian sector, the risk of harming participants by putting them through stressful simulations remains a concern. Good practice suggests aiming for moderate levels of stress (to encourage memory formation) while ensuring that simulation scenarios are clearly linked to specific learning objectives, and participants are encouraged to focus on how they react to stressors to learn more about their own responses to stress.

While the risk of harm cannot be removed completely, experienced training providers have put in place safeguards. These include having a qualified psychologist administer confidential pre-training psychological and trauma history questionnaires and providing consultations with participants of concern prior to the training. An onsite psychologist can also be made available to support participants during simulations. All trainers, learners and actors should feel empowered to step out of a simulation at any point if they feel it is beyond them to manage. Finally, a psychologist can follow up with any participant who struggled in the training to ensure their wellbeing. Overall, any stress-inducing simulation should aim to have well-trained role players, psychological support personnel and clear guidelines and rules.

i Turner, C.R., Bosch, D. and Nolty, A.A.T. (2021) 'Self-efficacy and humanitarian aid workers' *Journal of International Humanitarian Action* 6(1), 1–12 (https://doi.org/10.1186/s41018-021-00092-w) and Roberts, N.T. (2021) *Hostile environment awareness training for humanitarian aid workers: an outcome evaluation*. Doctoral dissertation, Fuller Theological Seminary, School of Psychology.
ii Arnsten, A.F. (2015) 'Stress weakens prefrontal networks: molecular insults to higher cognition' *Nature Neuroscience* 18(10), 1376–1385 (https://doi.org/10.1038/nn.4087) and McEwen, B.S. and Akil, H. (2020) 'Revisiting the stress concept: implications for affective disorders' *Journal of Neuroscience* 40(1), 12–21 (https://doi.org/10.1523/JNEUROSCI.0733-19.2019).

Security risk management training

In-person and online training courses in security risk management for humanitarian staff cover essential aspects of managing security, including how to identify risks and mitigate them, as well as how to respond to particular situations or crises, including detention and kidnapping. Increasingly, these courses are considering identity-based risks and how to incorporate these within security risk management.

Training tends to be externally provided, but some organisations have developed internal systems to train staff to become security focal points. Some of these courses have become part of a certification programme to formally recognise

the skills and competencies of security staff (see 'Further information' at the end of this chapter).

Specific training on different aspects of security risk management is also readily available, such as training on incident reporting, driving (defensive, safe and armoured vehicles), and crisis management; courses include tabletop exercises, which can cover multiple offices in different locations across an organisation. External service providers also offer crisis management courses, and guidance on how to develop and facilitate this type of training is available online (some examples are in 'Further information' at the end of this chapter).

There are examples of strategic training courses for senior leaders, such as security directors and senior leadership with security responsibilities, for example on duty of care and security risk management frameworks. However, security risk management training resources for senior security staff remain uncommon and most learning is shared through networking organisations and at events and workshops.

5.2.3 Challenges

Despite progress in the provision of security training to humanitarian aid workers, significant challenges remain – especially in personal safety and security training.

Table 9 Challenges in the provision of security training

Area	Challenge
Disparities	National aid workers, including those working for international organisations, are much less likely to receive personal safety and security training than their international counterparts.
Access	There is a lack of locally accessible and language-appropriate security training available, which makes it more challenging to provide resources to national aid workers. Limitations in the location and timing of courses can also hinder staff more generally from accessing training. Additionally, there are concerns that HEAT courses have come to be seen as the gold standard in security training, while not being financially or logistically accessible to most humanitarian aid workers, especially national aid workers.

Area	Challenge
Effectiveness	Despite a reliance on personal security training to prepare staff to work in high-risk locations – particularly HEAT courses – there is limited published evidence on the effectiveness of different types of personal security training. While published studies support the efficacy of such training, most reports of impact are anecdotal.
Costs	Security training can vary significantly in cost depending on what is provided to staff and where, with many security staff forced to make decisions over who gets trained and who does not, based on available funding.
Sustainability	Training courses tend to be one-off experiences. Even though some organisations require refreshers every few years, much of the information imparted is quickly forgotten without regular practice or a clear link to work responsibilities.
Quality	The absence of a clear standard for personal safety and security training means a wide variance exists between courses, both those provided within organisations and those provided by external service providers. Organisations with less knowledge of security risk management or fewer financial resources are more likely to inadvertently pick poorer-quality security training for their staff.
Relevance	Some security courses, particularly those provided online, lack tailoring to specific contexts, programmes, organisations and individuals. Although this makes the training more accessible, it also risks not being relatable to the trainees' particular needs and experiences.
Diversity	Although there has been progress in this area, there is still a lack of diversity in trainers, which can impact their ability to effectively engage with – and tailor content to – diverse groups of aid workers.

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

5.2.4 Good practice considerations

Organisations should make special efforts to ensure that all staff have access to security training and learning opportunities, but especially staff members most exposed to security risks. This means going beyond a simple assessment of training needs and carrying out an organisation-wide evaluation of risk levels of different staff, their access to security training and measures to cover identified

gaps. This can be complemented by the translation of training materials into relevant local languages. For some international organisations, this has meant reducing the provision of HEAT courses to free up funding for comprehensive personal security training for more staff – especially those who would normally not receive training.

Case example: Security as a right

One organisation's security team has focused on fostering an organisational environment that sees security as a right. This involves educating staff on what they should expect from the organisation in terms of security support and how to raise concerns if what is provided in practice does not match what staff have been told to expect. This is reinforced in training and through awareness-raising to empower staff to exercise their right to security.

Online training has become an important resource within the humanitarian sector. Increasingly, security training courses are available at cost and free, with differing levels of detail, covering multiple aspects of security, and in an increasing number of languages. The advent of artificial intelligence has sped up the process of developing and translating new online courses. While the generic nature and 'cookie cutter' design of online courses – especially those that are freely available – remains a weakness, these resources can serve as an introduction to security that can be complemented by more detailed and organisation-relevant training.

A challenge with designating security training by contextual risk levels is that it can lead to gaps in threat events, such as interpersonal violence, which are more likely to be covered in higher-risk personal training courses but are relevant to most staff, no matter their location. For this reason, some organisations and training providers have adopted a modular approach to training, designating certain topics as 'core' for all staff and building modules on top based on individual needs, location, threats, organisational identity and frameworks.

Some external training providers offer bespoke courses adapted to particular needs. These can be expensive. In-house training, while also a significant organisational investment in terms of funding and personnel, allows courses to

cover organisation-specific circumstances, such as the type of programming and any particular staff profiles, and have greater adaptability to particular contexts and challenges. Several resources exist to support organisations with developing in-house security training (see 'Further information' at the end of this chapter).

Several organisations have opted for a training of trainers approach, which allows them to build internal capacity and provide bespoke training in more locations. Such approaches struggle with quality control and must be closely monitored. Interagency collaboration and joint investment to provide context-appropriate security training courses to local aid workers have also proven useful and can reduce training costs.

In order to reinforce the learning imparted during training courses, some organisations have built in ongoing reference to safety and security issues in routine work and established periodic safety and security drills. For those with security responsibilities, some organisations have developed a mentoring programme and assigned 'homework' that relates to the trainees' actual responsibilities, allowing them to learn while doing their work. For example, one UN agency provides 90 days of on-the-job training for security personnel following its security course.

Inclusive security in training

Discussing differentiated risks based on identity profiles can be challenging. Training offers an opportunity to tackle myths and prejudices in this area, and several trainers have used the space to encourage staff to think beyond their own identity profiles. Below is a list of examples of how inclusive security has been addressed in training.

- Real-life examples from the group, anonymised and shared and discussed by the facilitator. It can be impactful to hear what colleagues face on a daily basis (including internal threats). Even if there is animosity to that particular profile, most individuals do not want harm to come to their colleagues.
- A role-playing exercise in which trainees are asked to consider the risks faced by imaginary characters with unique identity profiles in particular situations.

- The purposeful recruitment of diverse trainers, which offers trainees an opportunity to hear first-hand the security challenges particular identity profiles face. It can also be helpful for trainees to see similar profiles in positions of influence and respect (e.g. teachers). In general, a combination of trainer profiles (gender, ethnicity, background and skills, for example) is good practice. The diversity of trainers should aim to reflect the diversity of trainees.

One organisation's security training covers issues such as what staff with limited mobility can do at checkpoints or during crossfire, and how their colleagues can support them in these circumstances.

Table 10 Considerations for selecting training providers

Consideration	Factors
Profile	The training provider's values, motivation, ethics and culture align with the organisation and its staff. Ideally, training teams are put together considering all the skills and backgrounds required, including their ability to engage with humanitarian programme staff adequately.
Reputation and experience	Trainers are able to provide references and credible testimonials from other aid organisations, and have the capacity and experience to train humanitarian aid workers. Contextual experience is relevant when courses are in a particular geographical location. A teaching background or technical expertise in particular topics (e.g. sexual violence or trauma) can also be important.

Consideration	Factors
Content	The content of the security training aligns with the types of risks the organisation's staff are likely to face, and its overall security approach. It may be appropriate to seek training with simulation exercises, but these can be too aggressive or inappropriate for the staff being trained. The content covers relevant soft and hard skills. Some courses may focus on higher-impact and lower-likelihood risks, such as abduction, and may neglect lower-impact but higher-likelihood risks, such as interpersonal conflict and chronic stress.[i] More advanced courses may consider staff wellbeing and stress management, as well as identity-based risks. Many organisations include first aid training. This should be context-appropriate and provided by a trainer with the necessary qualifications.
Costs	A comparison of costs between different training providers is good practice but should also account for the quality and content of the training provided. Additionally, consideration should be given to whether it is more appropriate to train fewer staff members with higher-quality and more intensive security courses, or to choose a cheaper option that reaches more staff – especially those most at risk of experiencing a security incident.
Individual trainers' identities	It is good practice to consider trainers' individual skills, knowledge and experience, and whether particular trainers can be requested. Having a diverse team of trainers who reflect the profiles of the staff being trained (e.g. all genders and relevant ethnicities) can encourage greater participation and engagement.
Location and language	The location and accessibility of training are particularly important considerations, including the languages the training is available in and costs related to attendance.

[i] For more information on content considerations, see: EISF and InterAction (2014).

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

Case example: Trauma-informed training principles

One organisation that provides in-house personal safety and security training with simulation components has developed trauma-informed training principles for its course. These are:

- **Safety** – trainers take measures to ensure participants feel psychologically and physically safe during the training.
- **Trustworthiness and transparency** – trainers let participants know in advance what they should expect from the course, the simulations and the trainers; there are no surprises, and staff are informed in advance of topics that could be triggering.
- **Support and connection** – trainers make concerted efforts to engage with participants one-on-one, and participants work together in small groups; in-house counsellors are on standby during the course, and there are external counselling options for staff needing more support.
- **Collaboration and mutuality** – the course is designed to encourage sharing of experiences by participants.
- **Empowerment, voice and choice** – the course covers good practice (rather than 'do's and don'ts') and encourages participants to examine what may work for them in different contexts; participants can remove themselves from a scenario that feels unsafe or that crosses their own personal boundaries.
- **Social justice** – the training recognises the power dynamics between individuals, and specifically speaks to issues of identity and risk; in order to avoid perpetuating harmful stereotypes, fictional locations used for the training do not resemble real-life contexts or people.
- **Resilience, growth and change** – the course is meant to increase confidence among participants by making them feel safe, supported and validated; teaching methods validate participants' responses; all simulations have debriefing sessions afterwards where participants reflect on what worked for them and what did not.

Further information

Guidance

EISF and InterAction (2014) *NGO Safety and Security Training Project: how to create effective security training for NGOs* (https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos).

GISF (2022a) *Security and safety training pack* (https://gisfprod.wpengine.com/long-read/security-safety-training-pack/).

GISF (2022b) *Inclusive security session plan.* Security and safety training pack (https://gisf.ngo/long-read/security-safety-training-pack/3-training-resources/).

GISF (2023) *NGO crisis management exercise manual: a guide to developing and facilitating effective exercises* (www.gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/).

GISF (n.d.) *1. Security training.* NGO Security Toolbox (www.gisf.ngo/toolbox-pwa/resource/1-field-security-training/).

ICRC (2021) *SAFE: security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Research and discussion

Arnsten, A. F. (2015) 'Stress weakens prefrontal networks: molecular insults to higher cognition' *Nature Neuroscience* 18(10), 1376–1385 (https://doi.org/10.1038/nn.4087).

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/).

Breckenridge, M.-J. et al. (2023) *Aid worker security report 2023 – Security training in the humanitarian sector: issues of equity and effectiveness.* Humanitarian Outcomes (www.humanitarianoutcomes.org/AWSR_2023).

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

Headington Institute (psychological support and research on HEAT): https://headington-institute.org/

McEwen, B. S. and Akil, H. (2020) 'Revisiting the stress concept: implications for affective disorders' *Journal of Neuroscience* 40(1), 12–21 (https://doi.org/10.1523/JNEUROSCI.0733-19.2019).

Roberts, N. T. (2021) *Hostile environment awareness training for humanitarian aid workers: an outcome evaluation.* Doctoral dissertation, Fuller Theological Seminary, School of Psychology.

Turner, C. R., Bosch, D. and Nolty, A. A. T. (2021) 'Self-efficacy and humanitarian aid workers' *Journal of International Humanitarian Action* 6(1), 1–12 (https://doi.org/10.1186/s41018-021-00092-w).

UNDSS (2021) *Best practices for inclusive security training* (https://gisf.ngo/wp-content/uploads/2021/04/UNDSS_Best-Practices-for-Inclusive-Security-Training.pdf).

Training resources

DisasterReady: www.disasterready.org/

GISF: https://gisfprod.wpengine.com/training-events/

IFRC: https://ifrcstaysafe.org/stay-safe-e-course

INSSA: https://inssa.org/certification

Kaya: https://kayaconnect.org/

UNDSS: https://training.dss.un.org/thematicarea/category?id=6

5.3 Security communication within the organisation

In the complex environments where aid organisations operate, effective communication of security information is not just a procedural necessity: it is also a critical component of protecting staff and ensuring the continuity of humanitarian work. The better informed a staff member is, the more likely they are to understand and comply with the security risk management processes put in place by their organisation. Moreover, well-disseminated and high-quality information can help alleviate the anxiety and uncertainty that often accompany work in volatile or high-risk environments.

5.3.1 Person-centred communication

A key principle in the dissemination of security information is to adopt an approach that is both person-centred and audience-specific. Unlike traditional models that may focus on the organisation's needs, this method prioritises the specific concerns, vulnerabilities and requirements of the individuals at risk, while also tailoring the communication method to the target audience. Whether the information is shared individually through briefings or collectively via intranet pages or SMS alerts, content and delivery should be adapted to suit the recipients. This approach not only ensures compliance with security protocols, but also actively engages staff by making the information relevant to their immediate circumstances and personal security.

For instance, when briefing an individual staff member about risks in a high-risk environment, it is crucial to consider factors such as their background, experience and role within the organisation. A generic briefing might not sufficiently address the particular risks faced by a female staff member travelling alone in a conservative region, or a staff member with health vulnerabilities. When addressing larger groups via Intranet or SMS alerts, the information should be clear, accessible and tailored to the common concerns of the group, while still allowing for individual considerations where necessary.

Security staff need to be creative about how they share information.[84] Language, formats and channels all need to be considered. Visual aids like infographics,

84 Storytelling, for example, can be an effective way to engage staff in security training courses. For more, see Persaud, C. (2022) *Storytelling for learning: using engaging, ethical stories for effective security training.* GISF (https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/).

maps and flowcharts can help make complex information easier to digest, and plain language, clear instructions and avoidance of technical jargon can significantly enhance the effectiveness of communication.

Ultimately, the goal of security communication is not merely to inform but to empower. Staff need to be able to understand not only what they need to do, but also why it is important as this increases the likelihood of compliance and helps to build a positive security culture. By providing staff with the targeted information they need to understand and navigate the risks they face, organisations can help them to work safely and effectively, even in the most challenging circumstances.

▶ *See Chapter 1.2 for more on a person-centred approach to security.*

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

5.3.2 Modes of information dissemination

The effectiveness of security information dissemination largely depends on the channels and methods used.

- **Organisational webpages for staff (intranet).** Intranets are a valuable tool for disseminating security information. Organisations can use the intranet to post regular updates on the security situation, changes in risk levels and updates to security protocols. There may also be specific pages providing guidance to staff with particular identity profiles. However, intranet relies on functioning networks, which might not always be available for all staff.
- **Email.** Email remains a key channel for disseminating information within aid organisations. To be effective, emails need to be clear, concise and structured, with important information prominently displayed. Urgency indicators, such as priority flags and clear subject lines, help ensure that critical messages are not overlooked. Regular updates are crucial in ongoing situations, while translation into staff members' primary languages avoids misunderstandings (sometimes providing links to AI translators can be sufficient). It may be beneficial in some circumstances to request that staff confirm receipt and understanding of emails, particularly for critical communications.
- **Mobile phone alerts (such as SMS or apps like Signal and WhatsApp).** Alerts sent to mobile phones provide a direct and immediate means of communication, ensuring that critical information is delivered to staff even when they are travelling or working remotely. These alerts are particularly useful in scenarios where rapid dissemination of information is required, such

as during a sudden escalation in violence or an unexpected disaster. However, it is crucial to balance the frequency of alerts to avoid overwhelming staff with excessive messages, which could lead to important alerts being overlooked.

- **Briefings.** Travel-related briefings are an essential part of security information dissemination, especially for staff members who are about to enter a volatile or unfamiliar environment. As situations can change rapidly, it is important to provide updated security briefings regularly to affected staff. Briefings should never be a one-off event.

▶ *See Chapter 7.1 for more on guidance on briefings and travel-related risks and mitigation measures.*

- **Situation reports (sitreps).** Sitreps are a crucial tool for keeping staff informed of the prevailing security situation. These reports should be able to be produced quickly, be concise and focus on providing up-to-date situational information that is easily digestible. A well-crafted sitrep not only outlines the current security environment, but also highlights potential implications for the organisation's operations and any changes that may be required to procedures.

  Sitreps have a fairly familiar format, but should still be tailored for their audience and purpose. Sitreps for project staff focus on actionable advice and immediate risks, while those written for senior management might include a broader analysis of trends and potential future scenarios.

- **Reports.** In addition to more immediate updates provided by sitreps, organisations may produce analytical reports that offer a deeper examination of security trends and risks. These reports can be triggered by significant situational or contextual shifts and are designed to inform strategic decision-making within the organisation. Analytical reports can also be time-bound, such as monthly or quarterly assessments, and may include a range of media and other resources.

  While these reports are less likely to result in immediate procedural changes, they play a critical role in shaping the organisation's long-term security strategy. For example, a report might highlight emerging threats in a particular region that could affect the organisation's future operations, leading to a review of risk assessments and contingency plans. Given the strategic nature of these reports, it is essential that they are written with the intended audience in mind. Senior management, for instance, may require a more detailed analysis of the potential impact on operations, while operational staff might benefit from summaries that focus on the practical implications for their day-to-day activities.

► *See Chapter 4.4 for more on analysis of security incident trends.*

► *See Chapter 3.4 for more on security monitoring mechanisms.*

5.3.3 Managing information overload

One of the significant challenges in security information dissemination is the risk of information overload, particularly in volatile environments where events can unfold rapidly. In such situations, the sheer volume of information can overwhelm staff, making it difficult for them to absorb and act on the most critical updates. A triage system prioritises information based on its urgency and relevance.

The triage system should be guided by a series of key questions and considerations:

- **Operational importance.** Will the safety and security of staff be compromised if this information is not passed on immediately? If yes, share immediately. If not, consider the point(s) below.
- **Situational update.** Does the information indicate a potential effect on security, possibly indicating the need for heightened precautions? If yes, inform relevant staff in a timely manner. If not, consider the point below.
- **Context shift.** Does the information indicate a trend or other longer-term implications for the programme environment? If yes, consider when and how best to use the information to inform strategic decision-making.

Each organisation will need to consider the best way to transmit security information for each level, and ensure staff are trained on how and when to share this information, and with whom.

For information that has immediate importance and represents a broad threat to staff members, the priority is to disseminate as quickly and widely as possible. Traditional security communication methods, such as a communications tree, can be effective in these scenarios, but many organisations now also use broadcast or group messaging. These methods allow for rapid dissemination of critical information, ensuring that all relevant staff are informed and can take appropriate action without delay.

Examples of a triage information-sharing system

- **Operational importance**. A protest outside the country's parliament buildings is turning violent. Inform staff to avoid the area. Use SMS, a communications tree, broadcast or WhatsApp/ Signal group to quickly disseminate information to staff working in the area.
- **Situational update.** Protests are planned in the next few days outside of the parliament buildings. Send out an email advisory and/or incorporate into sitreps, specific security reports and SOPs.
- **Context shift.** Protests brought in a government that is hostile towards humanitarian organisations. Incorporate information as relevant into security reports, briefings or training, and feed into security analytical processes.

Communications tree

A communications tree is a hierarchy system used to quickly disseminate information to a large group. It begins with one person contacting key individuals, who then each inform others, creating a cascading effect until everyone is reached. This model is ideal for emergencies or urgent updates, ensuring rapid communication. Communications trees can be manual, involving direct calls, or automated, using software to send messages via calls, texts and emails.

For communication at the operational level, introducing redundancy is essential. This means that staff have access to multiple, independent methods of communication, such as radios and satellite phones, so that communication can continue even if one method fails.

▶ *See Chapter 6.1 for more on different communication methods and developing communication plans that introduce redundancy.*

For situational updates or shifts in context that do not require immediate action but have longer-term implications, a more measured approach is often appropriate. These types of updates should still be communicated promptly, but the emphasis should be on providing a thorough analysis of the situation and its potential impact on the organisation's security risk management.

High-level strategic updates might be best communicated through formal reports or executive briefings, while operational updates could be disseminated via more informal channels such as team meetings or group chats. More in-depth concepts and security information could be shared in briefings and training sessions. The key is to ensure that the communication method aligns with the urgency and importance of the information, as well as the preferences and habits of the intended audience.

Dashboards and apps

Aid organisations are increasingly using dashboards and customised mobile apps to share security information.

Dashboards provide a platform for staff to access security-related information, such as security plans, often in visually engaging ways (such as heat maps) (*see Chapter 3.4 for more on dashboards*).

Mobile apps can deliver real-time security updates, enable rapid incident reporting and offer guidance on specific security situations (such as actions to take at checkpoints). They can also include emergency contact information. Apps can be particularly useful for staff who need access to security information on the go.

Verification and prudent overreaction

The accuracy and reliability of security information are of paramount importance. There is, of course, an expectation that all information disseminated by the organisation has been verified to the best extent possible. However, in rapidly evolving situations it may not always be feasible to fully verify information before it needs to be communicated. In such cases, the concept of prudent overreaction comes into play.

Prudent overreaction involves taking precautionary measures based on the available information, even if it has not been fully verified, provided that the potential risks justify such an approach. For example, if there is an unverified report of an imminent security threat in a particular area, it may be prudent to temporarily suspend operations or advise staff to take shelter until more information becomes available. The key is to communicate the information in a way that clearly outlines the reasons for the measures taken, while acknowledging the uncertainty surrounding the situation. When conveying such information, it is essential to anticipate likely questions staff might have, such as 'Why do I need to know this? and 'What do I have to do?'. By addressing these questions upfront, organisations can help reduce confusion and ensure that staff are prepared to take the necessary action in response to potential threats.

Continuous review and adaptation

Effective security communication within aid organisations relies heavily on continuous feedback and adaptation. Security staff should actively seek and incorporate feedback from colleagues to ensure the information provided is both clear and useful. As security environments and threats evolve, so too must the communication strategies and methods used. Regular reviews or audits of these practices, involving input from all organisational levels, are essential. Staying informed about new communication technologies can help improve the efficiency and reach of security updates.

Further information

Persaud, C. (2022) *Storytelling for learning: using engaging, ethical stories for effective security training.* GISF (https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/).

5.4 Staff care

Resilient staff and teams are crucial to a resilient organisation. In the often high-stress environments of aid work, adequate support for the mental and physical wellbeing of staff enhances this resilience and the ability of staff to make the sound decisions critical for effective security risk management.

This chapter focuses on the importance of integrating physical and mental health considerations into security risk management and supporting staff before, during and after critical incidents. It provides strategies for maintaining staff wellbeing and strengthening mental health and psychosocial support to avoid long-term adverse outcomes. The outlined approach can be implemented by non-medical staff, ensuring that all aspects of staff care are addressed effectively.

► *This chapter focuses primarily on mental health. For physical medical considerations and necessary preparations, see Chapter 5.5.*

5.4.1 Key concepts

Resilience and wellbeing

Resilience is 'the process and outcome of successfully adapting to difficult or challenging life experiences, especially through mental, emotional, and behavioural flexibility and adjustment to external and internal demands'. Addressing resilience involves supporting overall wellbeing to build both individual and team capacity to handle shocks effectively, while also providing immediate and long-term psychosocial support in response to incidents (see Figure 11).

The resilience of staff members in the face of challenging environments and events may depend on various factors, including the strength of social networks, cultural and other identity factors, general outlook and disposition and coping mechanisms. Capacities for resilience can be developed and nurtured, and each individual has their own level of resilience influenced by personal characteristics, expectations, lifestyle and self-awareness of their limits. The work environment also plays a role, with factors such as working hours, expectations, workload and potential vicarious trauma affecting resilience.

Figure 11 Factors supporting resilience

While many stressors may be beyond their control, organisations can still foster resilience by promoting a supportive work culture.

In a humanitarian response, living conditions are often challenging, whether staff are residing in a crisis-affected area or in shared organisational housing or tents. For staff working away from their home and families, stressors outside office hours can be more significant as they lack familial support. Staff may struggle with blurred boundaries between work and personal time, and may experience heightened stress due to limited access to family support. Staff who are resident in the location might face additional pressures as members of the affected community, with crises potentially impacting their families and friends and surrounding infrastructure.

Implementing a team-based peer support approach and ensuring that managers understand the importance of self-care and mental health risks can significantly enhance both individual and organisational resilience.

A person's overall wellbeing is more than physical health and safety, and the extent to which security risk management considers and actively supports the mental, emotional and social dimensions as well can make a critical difference to morale, performance, decision-making and personal outcomes. Well staff make better security decisions and are better able to weather stressful environments and incidents.

Case example: Focusing on healthy coping mechanisms

An organisation has included stress management in its personal health, safety and security training for all staff. During this session, staff learn how to recognise signs of stress in themselves and others and discuss their coping mechanisms. They each commit to at least one healthy coping mechanism that they are going to focus on in the months after the training. The session wraps up with participants agreeing on actions the organisation can take to improve staff wellbeing. Examples include introducing plants to the office, arranging to have a medical doctor on site for one day a month for walk-in consultations, organising a team breakfast once a week, and creating a safe space for staff to decompress during or at the end of their workday. Sessions help to normalise conversations about wellbeing and health, create better understanding about how teams can support each other and increase awareness of staff members' own coping mechanisms.

A person's overall wellbeing has been described as comprising six dimensions: physical, emotional, social, intellectual, professional/occupational and spiritual/religious. These dimensions are interdependent, meaning that if one area is affected, it can impact others. Security staff need to understand and account for these various dimensions and their interrelatedness, especially during challenging events or periods. Security staff can also play an important role in advocating for organisation-wide implementation of wellbeing initiatives that address these six dimensions.

Wellbeing practices in the workplace

Wellbeing practices in the workplace can include appointing a wellbeing focal point or committee to organise fitness activities, workshops and training on stress management and mental health. Practices such as promoting gratitude and recognition and encouraging breaks can boost morale and productivity. Policies such as no emails after work hours, encouraging staff to take annual leave and offering flexible work arrangements further support wellbeing. Providing spaces for meditation, yoga and social activities can help employees feel valued and supported. Offering professional development, financial literacy programmes and support for staff in special circumstances, such as new parents or those with religious commitments, can all promote wellbeing.

Stress and trauma

Because of what they do and the environments they are in, all aid workers are vulnerable to stress. This includes security professionals and leaders who must regularly deal with incidents affecting others. Different individuals will experience and manifest stress in different ways and develop individual coping mechanisms, depending on their personal profiles and circumstances.

There are different types of stress, and stress can be healthy or unhealthy. Healthy stress helps people focus on the task or situation at hand, mobilises energy and prepares them for action. For example, having a deadline can cause someone to be stressed, but can also help to get a task completed. In situations of tension or risk, stress and fear reactions can give people the focus they need to survive.

When stress occurs too often, however, or is too intense or lasts too long, it becomes harmful. All stress uses energy. A seemingly endless series of tight deadlines or continued exposure to high-risk situations or experiences can deplete energy reserves. When several stressors occur at the same time and especially when these are prolonged, including corrosive stressors like ongoing fear, uncertainty, and conflict, this can lead to cumulative stress.

There is a difference between stress and trauma. Regular stress responses, called acute stress, like the 'fight-or-flight' survival mechanism, are deactivated when the threat is over. With trauma, the body stays in that survival mode and continues to respond as if it were under threat even after the threat is over. Traumatic events overwhelm people's ability to cope and manage stress.

If a person is suffering from a continued level of increased stress, their coping mechanisms may be overwhelmed, reducing their ability to withstand the psychological impact of a traumatic event. Long-term stress and trauma will also affect a person's decision-making ability.

Trauma may be the result of an acute stressor (such as a critical incident or life-threatening event), cumulative stress or continued exposure to others' trauma. Although trauma is common, a single or even a series of adverse events does not inevitably result in trauma. Rather, it depends on how a person responds and is equipped to deal with the experience, which links closely to the resources at their disposal as well as their past experiences.

The range of stressors that can result in trauma is very wide and this trauma can occur hours, days, weeks, months and years after (the start of) an occurrence. These stressors can vary in intensity and may result in post-traumatic stress disorder (PTSD) or other forms of trauma. In all cases, they impact a staff member's resilience. Organisations may need to be prepared to provide support long after an event has occurred.

Indirect trauma

There are several ways in which aid workers can suffer trauma indirectly. Secondary traumatic stress refers to symptoms like nightmares or anxiety that emerge from an individual's indirect exposure to another person's trauma, typically through their interactions with or assistance to the trauma survivor. Vicarious trauma involves a profound change in one's worldview caused by repeated indirect exposure to others' trauma. It commonly affects first responders such as paramedics, but can also affect others, for example media and communications staff repeatedly exposed to distressing online content.

5.4.2 Security, mental health and psychosocial support

The risks of mental health impacts associated with humanitarian aid work must be recognised as part of an organisation's duty of care. Developing localised strategies can improve the working environment and bolster preparedness for psychosocial response to support staff during and after emergencies and critical incidents. This can be guided by a mental health and psychosocial support (MHPSS) approach, which addresses both the mental health needs and the social factors affecting the wellbeing of individuals and groups by integrating psychological care with social support systems. Note that, while psychological support focuses on individual therapy and managing mental health issues like anxiety or depression, psychosocial support is a broader approach that integrates both psychological and social aspects of wellbeing, addressing the impact of relationships, environment and community on mental health.

Incorporating MHPSS resources into security risk management processes enhances staff resilience and reduces the risk of incidents related to stress or burnout. This can involve:

- Fostering a supportive culture that reduces stigma and encourages staff to seek help before issues escalate and compromise security.
- Identifying MHPSS needs and barriers.
- Mapping organisational and local mental health services and psychosocial support providers, vetted by clinicians.
- Developing strategies for the recruitment, selection and oversight of psychosocial support services.
- Connecting with local resources to enhance the management of critical incidents by providing immediate, culturally relevant psychosocial support.
- Including psychosocial response procedures within security and crisis management plans.
- Training leaders and managers on effectively responding to psychosocial issues, including mental wellbeing and resilience-building strategies.
- Preparing and training staff for trauma-informed psychosocial responses to critical incidents, including sexual violence.
- Incorporating mental health considerations into security training and briefings.

▶ *See Chapter 5.2 for more on how to incorporate mental health considerations into security training.*

Some experts recommend a mental health risk management approach, which treats psychological risks as one would security risks – using the same tools and frameworks – by assessing psychological risks alongside physical security risks and putting in place relevant mitigation measures and contingency plans. By embedding mental health into the security risk management framework, organisations can enhance overall resilience and effectively manage both security and psychological risks.

This can be supported by an initial mapping of the MHPSS needs and capacity in each organisational location. This mapping can consider the common stressors of staff with different profiles, as well as existing mental health issues and needs among staff members. It can include a review of what services, providers, facilities and programmes are locally or remotely available (including insurance plans) and to whom (considering, for example, staff language and accessibility needs). Prevalent attitudes and organisational culture and coping mechanisms towards stress, burnout, vicarious trauma and post-incident traumatisation are also important considerations.

The information gathered from this mapping can be used to inform an organisation's psychosocial support and wellbeing initiatives. The following are some examples of MHPSS services, both formal (through external and internal professionals) and informal (such as peer support groups).

Counselling and therapy services:

- Employee assistance programmes (EAPs) (third-party confidential counselling and support services for personal and work-related issues).
- Onsite mental health professionals (internal or external).
- Telehealth services (internal or external).
- Specialist services, such as psychiatrists or therapists, brought in following an incident or crisis.

Other initiatives include:

- Mental health workshops and training.
- Stress management programmes.
- Psychological first aid training.
- Peer support programmes.
- Online mental health resources.

It is important to regularly review MHPSS support options to ensure they align with staff needs and expectations and are relevant for – and accessible to – staff with diverse cultural backgrounds. Good practice suggests not relying solely on one support mechanism, but offering a variety of options relevant to different types of stressors and events, to effectively address the broad spectrum of staff needs. Finally, what is provided in terms of MHPSS needs to be clearly outlined in advance by the organisation, so staff know what services they have access to and what kind of support they can expect following a critical incident.

Case example: Wellness days

After the May 2023 escalation in Gaza, where staff had gone through an intense period of air strikes, an organisation provided all Gaza-based staff with two wellness days. Most staff had plenty of leave to take, but the wellness leave was intended as recognition and staff felt motivated and cared for. The office remained open for staff whose preferred coping mechanism was to be with colleagues.

5.4.3 General response considerations

Good practice in approaches to post-incident staff care and follow-up care covers a range of practical considerations.

Ensuring staff feel supported

In the aftermath of an incident or other stressful event, it is important for staff to feel the organisation understands that their experience has been difficult, and that it intends to support them and ensure that the next steps are as seamless as possible. Organisations can do this by listening to affected staff, supporting their post-incident needs and providing answers to initial questions, while connecting them with the necessary resources. Staff may benefit from time to process events and emotions surrounding the incident or situation. Organisations should encourage those involved to take time to rest, practise self-care and connect with loved ones. It is not uncommon for staff to have immediate physical or mental health needs following a stressful event. A structured response for supporting mental health directly after an incident, incorporating peer support and compassionate leadership and management, will reduce the likelihood of an individual needing professional support for trauma later on.

General staff care considerations during or following incidents or highly stressful events include the following:

- **Staff support messages.** When staff face hardships, receiving supportive messages from senior leadership (in their first language) can be impactful. Personal outreach from colleagues can also provide comfort. Communication can be via text, social media, email or phone, and can include opportunities for affected staff to respond to messages and share their experiences.
- **Hospital visits.** If a staff member is hospitalised away from home, arranging for another staff member or partner organisation to visit can alleviate feelings of isolation.
- **Care packages.** Customised care packages for staff affected by incidents or conflict can be delivered by staff, or through partners if the organisation is unable to access certain areas.
- **Reception team.** Having a reception team to welcome staff arriving in a safe location can make a significant difference. This team can be present to assist staff arriving from evacuations, critical incidents or violent situations.
- **Post-incident information.** Provide a written summary of available support, resources, insurance, benefits and legal advice to staff affected by an incident. This can be accompanied by personal guidance from a representative and a clear contact person for follow-up questions.
- **Post-incident psychological debrief.** Responsible staff can schedule a post-incident psychological debrief with a licensed psychological professional or other trained individual (see below).

▶ *See Chapter 4.4 for more details on post-incident debriefs.*

During relocation and evacuation

Organisations can take steps to ensure staff feel supported following relocation or evacuation, for example by ensuring their immediate needs are met (essential supplies, medical care and assistance with communication). This includes ongoing support during their stay at a safe location, such as regular check-ins, help with onward travel arrangements and access to medical and psychosocial services. The goal is to ensure staff feel safe, supported and connected throughout the relocation and evacuation process.

Survivor-centred approach

Whether supporting staff involved in a severe traffic accident, sexual assault, relocation from a life-threatening situation, abduction or another stressful event, organisations benefit from adopting a survivor-centred approach.

Key concepts of survivor-centred care are as follows:

- **Respect.** Honour the survivor's wishes and choices, treat them with dignity and understand that their reactions may be emotional, and may differ from others' expectations.
- **Confidentiality.** Share personal information concerning the survivor only on a 'need-to-know' basis and seek consent before disclosing any details beyond this.
- **Autonomy.** Recognise the survivor's right to make their own decisions, considering that autonomy may be interpreted differently in different cultural contexts. Provide clear information about procedures and potential outcomes to support informed choices.
- **Clarity and navigation.** The survivor may be disoriented after the incident and may require guidance to understand what they may need assistance with and how to access support.

The individual may be overwhelmed by the experience, and by the expectation to make decisions, so providing support through this process is critical. A survivor-centred approach prioritises the survivor's needs without unduly burdening them with employment questions, legal action, insurance procedures and having to navigate internal and external support mechanisms. This means providing a clear and concise overview of the benefits and support available and a designated contact person throughout the recovery period. In the early stages, this can be a member of the incident management team or survivor supporter. In the medium to longer term, this support (emergency leave during the period they are unable to work, return to work or career pathway changes for example) can be handed over to a supervisor, with regular support from a human resources manager, business partner or legal counsel, for example.

Responsible staff need to recognise that preferences for support can differ. For some, being supported may mean having someone to share their experiences with. Others may appreciate the opportunity to stay busy or focus on other things. Some will want to take the lead in all follow-up actions and responses, while others may have limited capacity or ability to do so and need more

organisational support. An external survivor advocate can be contracted to support survivors/affected staff.

A survivor-centred approach is distinct from a survivor-led approach, as there is some oversight to prevent decisions that could pose further risks. While deferring to the wishes of the survivor wherever possible, a survivor-centred approach allows for exceptions where their wishes might place them or others at risk of further harm.

5.4.4 Response actions

It is common for aid workers affected by critical incidents to experience a form of 'institutional betrayal' when their organisation, through actions or inaction, causes them further harm or even appears to side with the perpetrators. It is fundamental to ensure that staff feel cared for and heard following a critical incident.

Trauma-informed response

A trauma-informed response entails understanding the psychological and emotional impacts of trauma on individuals, and ensuring that responses prioritise their safety, wellbeing and empowerment, for example:

- **Safety** – ensuring the physical and emotional safety of affected staff.
- **Trust** – maintaining clear, transparent communication to build trust.
- **Peer support** – encouraging peer support from colleagues, family or others who have shared similar experiences.
- **Collaboration and mutuality** – fostering a sense of partnership and collaboration in the recovery process, recognising that healing is a shared effort.
- **Empowerment, voice and choice** – recognising individuals' ability to advocate for themselves and ensuring they have an opportunity to be heard.

- **Cultural, historical and gender considerations** – recognising that each individual's risk profile will be unique to them, and respecting cultural, historical and gender dimensions that may affect their recovery.
- **Avoid re-traumatisation** – being mindful of language and actions so as to prevent further harm.
- **Education and awareness** – educating relevant staff on the effects of trauma on affected individuals' health and behaviour, and how to provide an appropriate response.
- **Support for caregivers** – providing resources and support for caregivers as they are at high risk of secondary trauma.

▶ *For general guidance on incident response, see Chapter 4.4.*

▶ *For more detailed response guidance for incidents of sexual violence see Chapter 7.7.*

▶ *For more detailed guidance on responses to abductions see Chapter 7.9.*

Initial considerations and actions

Immediately following an incident, it is good practice to ensure the physical safety of the staff member by relocating them to a secure environment and, if needed and appropriate, providing first aid (including psychological first aid) and access to professional medical care (physical and psychosocial services). This should be closely followed by the development of a tailored personal safety plan.

Because the medical and psychological impacts of the incident might not be immediately apparent, options for support should ideally remain accessible long after an incident has taken place.

Psychological first aid and peer support

Peer support can be an effective mechanism for helping staff navigate difficult periods and events by fostering a sense of shared understanding and mutual aid. This approach enables staff to provide immediate emotional and practical support to distressed colleagues. Creating a supportive network can be particularly valuable in situations where professional psychosocial support may not be immediately available. Peer support not only enhances resilience, but also promotes a culture of compassion and solidarity within the organisation.

Organisations should ensure that all incident responders, including senior and executive leadership, facilitate peer support and compassionate leadership. All staff should be familiar with the Psychological First Aid (PFA) principles (see the box below), and everyone likely to interact with colleagues during and after critical incidents should receive basic PFA training.

Psychological First Aid principles

The three main principles are:

- **Look** – look for signs of distress or someone who may be in need of focused support.
- **Listen** – approach the person who may need support and ask for permission to help; listen to them, try to help them feel calm, and help them prioritise urgent needs; respect confidentiality and their autonomy.
- **Link** – give practical information and help link the person with support (within the organisation as well as loved ones as appropriate).

PFA focuses on addressing immediate needs and alleviating distress by providing compassionate support designed to help individuals cope with the emotional and psychological impact of a traumatic event. It is not a treatment for PTSD or other psychological conditions. It focuses on providing comfort and reassurance, actively listening to individuals' concerns, and offering practical assistance to address immediate needs such as finding safe shelter or medical care. PFA aims to validate the individual's feelings, helping them understand that their responses are typical given the circumstances. It involves connecting people with support networks, additional resources and professional support services as necessary.

To be effective, responders should be sensitive to cultural, ethnic, religious, language, sexual orientation and gender identity considerations that can impact an individual's experience of trauma and their recovery needs.

Other forms of peer support include support groups, mentoring, buddy systems and online forums for current and former aid workers.

Personal safety plan

Personal safety plans in the aftermath of a traumatic incident identify ways to stay safe or to mitigate additional harm, tailored to the survivor's specific physical and psychological safety needs. The components of a safety plan will vary depending on the incident, staff member and organisation in question. However, it can broadly include:

- Immediate safety measures, such as relocation to a 'safe haven', establishing means of communication and emergency contacts.
- Physical security measures, such as secure accommodation and other forms of support, including the presence of a trusted friend or colleague.
- Risk assessment of the threat and any ongoing vulnerability of the affected staff member.
- Measures to stay safe at home (e.g. locks, emergency alarm, code for opening doors).
- Measures to stay safe in other locations, such as at work and in public.
- Ensuring access to important documents such as passport, driver's licence, ID card and ATM card.
- Guidance on what to do if there is contact with the perpetrator, if applicable.
- How to cope with mental and emotional triggers.
- Contact information in case of emergency.

This can be followed by linking the affected staff member with relevant resources, including medical and psychosocial support (internal and external). In the longer term, organisations can consider developing a support plan with the affected individual that gives them clarity on the support available to them, benefits, insurance and long-term care.

Short-term actions

Once immediate needs have been addressed, it may be advisable to carry out a more detailed assessment of the affected staff member's safety, implement adaptations to their work assignments, review options for legal and justice measures (such as reporting the incident to the police), report the incident using organisational protocols and undertake a psychological debriefing. Be mindful also of the needs of caregivers and those providing support to the affected individual.

Psychological debriefing

Following an incident or event, it may be advisable to organise a psychological debrief – a structured, facilitated discussion designed to help individuals process the event and begin to manage their emotional responses. This typically involves gathering together those affected by the incident to discuss what happened and share their reactions and feelings, and arranging support from peers and mental health professionals. The goals of psychological debriefing include:

- helping individuals make sense of the event and their reactions to it;
- normalising their emotional responses;
- providing information on stress reactions and coping strategies; and
- identifying individuals who may need further support.

Debriefing is generally offered within 24 to 72 hours after the event to allow participants to express their initial thoughts and feelings while the event is still fresh. Some experts suggest that psychological debriefing should not be mandatory, as not everyone benefits from discussing the incident immediately, and for some it could exacerbate their distress. That said, beliefs and the tough-minded or stoic culture prevalent in the humanitarian sector, along with specific cultural attitudes, can sometimes make admitting the need for psychosocial support seem like a weakness. To address this, offering an initial psychological debriefing following an incident as an 'opt-out' rather than an 'opt-in' can significantly increase participation. Additionally, staff may worry that acknowledging psychological injuries could negatively affect their job prospects. Providing staff with reassurance that seeking support will not jeopardise their employment opportunities can help address this.

Supporting the supporter and others affected

The focus during and after most critical incidents is on survivors, but support should also extend beyond the immediate affected staff member and may include offering assistance to witnesses and the broader team. Those responding to an incident (at any level in the organisation) may require dedicated support. Cumulative stress and vicarious trauma are important considerations, especially for those providing support in one incident after another.

Individuals in need of additional support can be offered time off to recover, access to psychosocial support and assistance in managing their workload outside of the incident. Other effective interventions include offering access to mental health resources, such as counselling and support groups, stress management

workshops and fostering a supportive work environment where staff can discuss their concerns openly. Regular check-ins and creating opportunities for staff to engage in mindfulness practices or relaxation techniques can help manage stress and prevent burnout, ensuring that all employees are equipped to handle workplace challenges and personal pressures.

Long-term aftercare

In the longer term it may be advisable to continue monitoring the staff member's wellbeing through regular check-ins, adapting the safety plan as necessary, and ensuring they have access to sustained psychosocial support and medical care, including trauma-informed therapy if necessary. This can be documented in a detailed support plan. At this point, it can also be helpful to provide more detailed guidance on legal and justice avenues, as well as considering return-to-work options.

General support plan

Depending on the severity of the incident, affected staff may require long-term aftercare. Responsible staff can develop a comprehensive support plan with the affected staff member. This should be flexible and survivor-centred, incorporating medical and psychological assessments and treatment, aftercare, work reintegration and transition to long-term services such as national health services. The plan should be sensitive and open to cultural factors and the affected staff member's preferred paths to recovery, which may include traditional healing methods.

Organisations should clearly outline the extent, cost and duration of support they are able and willing to provide following an incident, in order to manage expectations.

Long-term support for survivors and staff involved in severe incidents can additionally require:

- work duty adjustments;
- tactful communication about absences;
- regular check-ins to address ongoing concerns;
- notifying insurance providers, when appropriate and with consent;
- financial aid for affected individuals and support staff (e.g. response team members); and
- support for late-onset injuries (for example, PTSD or traumatic brain injuries).

It can be helpful – and for some organisations this is standard policy – to keep documentation of medical and other reports on the diagnosis of injuries to help guide long-term support.

Case example: Failures in aftercare

Following a severe critical incident, an international aid worker had to undergo multiple psychological and psychiatric assessments and submit eight reports before their PTSD diagnosis was accepted by their employer. Later reports included diagnoses of depression. Additionally, the staff member had to provide 12 medical reports before the organisation was willing to concede that their injuries were linked to a gunshot wound sustained during the incident. This process was not only difficult for the individual, but also caused other staff to lose confidence in the organisation's willingness to support them should they be injured while working in high-risk contexts.

Justice and legal redress

When staff who have experienced violence want to seek justice through formal legal mechanisms, organisations will need to be prepared to advise on their legal options, including the implications of reporting to local authorities and the legal definitions of the criminal offence in that context. Organisations should have a comprehensive understanding of the legal environments in which they operate, including which police station to approach in the event of an incident and any requirements for reporting (including timelines), and established relationships with trusted local legal professionals who can provide advance guidance and immediate assistance. If a staff member chooses to pursue justice, an organisation can consider the extent to which it is prepared to provide the following types of support (and how):

- Accompanying affected staff during police reports, interviews and evidence gathering.
- Securing appropriate legal representation.
- Providing practical information about arrest, court proceedings and potential penalties.

- Offering ongoing psychosocial support to help cope with trauma from legal processes.
- Clarifying procedures and timelines and ensuring staff can make informed decisions about prosecution.
- Having legal, medical and psychological services in place in the event of an incident, including forensic evidence collection.

Considerations when alleged perpetrators are staff members

In cases where the alleged perpetrator is a staff member – such as instances of sexual violence or other harm inflicted on another staff member – an organisation can consider the following actions:

- **Duty of care** – defining and providing legal, medical and psychosocial support to the alleged perpetrator, and determining when this support should conclude.
- **Internal investigation** – initiating an internal investigation to gather information to establish facts, ensuring sensitivity and neutrality, and involving trained, independent investigators.
- **Legal proceedings** – being prepared to support staff through legal proceedings and considering the consequences of involving local authorities; these are especially important considerations in contexts with severe punishment and poor incarceration conditions.

▶ *See Chapter 7.7 for more examples and considerations in the event of a sexual violence incident, as well as a more detailed discussion of internal investigations.*

Return to work

Returning to work following a severe incident can be challenging. It is important to recognise that reintegration is a process unique to each individual and may take a long time. The timing for the return to work should be flexible, acknowledging that some individuals may wish to resume their duties immediately, while others may need more time. This process should be managed sympathetically, possibly offering alternative roles or discussing retirement options if the individual chooses not to return. Organisations should ensure other staff members know

how to support returning colleagues, while also supporting them through any emotional impact the incident may have had on them.

5.4.5 Insurance and benefits

Overview of insurance

Organisations need to be prepared to cover the financial costs of responding to incidents affecting their staff. Most organisations do this by taking out insurance policies that cover a wide range of risks. However, some organisations have opted for self-insurance schemes, where the organisation assumes the financial risk associated with certain events, such as employee health benefits, workers' compensation or property damage, using its own resources to pay for claims.

It is important to remember that insurance cover provides compensation – not protection. It will not prevent disease or injury, but can help to mitigate the financial consequences of an incident. Insurance will also only cover the losses included in the specific terms and conditions of the insurer. Ultimately, what insurance companies provide is a level of economic protection, mitigating the impacts of negative events by transferring the risk of a large economic loss to the insurance company, in exchange for a premium.

Safety and security accidents and incidents can have major financial consequences for the staff concerned, their families and the organisation. There are immediate costs, such as medical evacuation and emergency treatment, which can quickly run into very large sums of money. There are also potential long-term costs, such as those resulting from permanent disability (for example following the loss of limbs) and long-term care needs. Some insurance policies provide for a risk management specialist to support a response, as well as covering costs for incidents such as illegal detention, evacuation due to insecurity, and abduction.

It is part of an organisation's duty of care to provide financial compensation to affected staff in case of injury, illness, death or during other life events. Since most organisations cannot cover these costs themselves, insurance coverage is their means to provide that compensation. For international organisations, this responsibility also applies to national staff. That some international organisations' insurance coverage does not extend to all staff members therefore becomes a serious operational and ethical problem. Insurance is a tool that can help fulfil an employer's responsibility, but should not usually entail the full extent of support that an organisation provides affected staff.

Aid workers should be informed of the details of the insurance coverage their organisation provides (with possible exceptions for special contingency policies – i.e. kidnap and ransom coverage). Staff have the right to enquire about the insurance coverage being provided to them and to seek more information. While psychological injury and disability may be included in medical and workers' compensation, it is not automatic. The organisation may need to ensure that these are covered, and not just assume they are, particularly if organisational documents specify mental health support.[85]

Case example: Access and eligibility assessment

One organisation has mapped out access to and eligibility for medical assistance and evacuation. As well as providing transparency to staff on coverage, this overview allows the organisation to identify insurance gaps and overlaps and improve equity.

The organisation first identified benefit groups:

- Country programme staff
- International staff
- Head office staff
- Remote telecommuters
- Non-staff guest travellers (e.g. board members)

For each group, the overview lists details on access to a medical assistance provider and applicable insurance cover:

- Access to medical assistance provider
  - Who?
  - When?
  - Information, advice and referrals? Yes/No
  - Routine/elective medical care?
  - Medical assistance for accident/illness? (e.g. Yes, Yes (while travelling internationally on official business))
  - Medical evacuation for accident/illness (e.g. Yes, Yes (while travelling internationally on official business))

85 Reilly, L. (2024) 'Is your mental health covered? Insurance for psychological injury'. Bond (www.bond.org.uk/news/2024/05/is-your-mental-health-covered-insurance-for-psychological-injury/).

  - What does the organisation cover? (Details on support provided at no cost and support for which costs will be incurred)
- Applicable insurance coverage
  - General information (on assistance with placing payment, submission of insurance claims)
  - Routine/elective medical care in country (e.g. local medical coverage, global health insurance coverage, none provided by organisation)
  - Routine/elective medical care out of country (per above)
  - Accident/illness medical care while travelling internationally on official business (e.g. business travel accident insurance, global health insurance)
  - Accident/illness medical evacuation while travelling internationally on official business (per above)

Gaps in – and absence of – national health insurance

Providing adequate support to national aid workers involves not only access to and eligibility for medical assistance, but also wider benefits such as psychosocial support coverage and access, life insurance, disability benefits, workers' compensation and paid training and development/education allowances. Evacuation support for national aid workers remains challenging, however, as it can involve much more negotiation with evacuation providers and requires visas and other administrative approvals in addition to the financial costs of insurance. In some instances, local insurance plans are either unavailable or unaffordable. Some international carriers can offer coverage to local nationals, although this depends on the country and insurance provider.

As no insurance at all is not an option, organisations can:

- Opt for a self-insurance scheme, if feasible, where the organisation sets aside funds to cover potential risks and claims instead of purchasing insurance from an external provider.
- Negotiate (global) insurance policy extensions.
- Provide a lump sum for medical coverage.

- Support requests for compensation or financial assistance in the case of disease, injury or death on a case-by-case basis.
- Develop an internal cooperative insurance system with an insurance pot created with a lump sum from the organisation, added to by contributions from participating employees.
- Provide free healthcare to all staff as a benefit of employment (as is often the case with medical relief organisations).

It is likely that, in countries prone to natural hazards, national medical insurance cover will not function in a time of crisis and alternative arrangements may need to be considered.

▶ *For more medical emergency considerations, see Chapter 5.5.*

Common insurance policies

Different organisations will have different insurance needs. Insurance should be considered a component of a mitigation strategy and, like everything else, requires a full appreciation of risks derived from a comprehensive assessment. Most organisations have insurance policies with the following types of coverage (noting that the following list is non-exhaustive):

- Standard health insurance.
- Standard accident insurance – including accidental death or dismemberment.
- Disability insurance – partial or total, long-term or short-term.
- Medical emergency insurance – including coverage for medical evacuation and emergency care in situ and in transit.
- War risk insurance – this is often a separate policy, or a supplement at an additional cost, covering injuries or deaths caused by 'acts of war or terror' (see more under 'Exclusion clauses' below).
- Special risk insurance – covering technical expertise for crisis management and contingencies to facilitate safe release of hostages.
- Business/general liability insurance – one of the most general insurance policies that insures against cost of third-party bodily injury or third-party property damage claims and, for instance, slip-and-fall cases on organisational premises.
- Auto liability and fleet/auto insurance – policies covering legal and financial responsibilities such as liability, collision and comprehensive coverage, as well as protecting against a broader range of risks, including damage to vehicles.

- Workers' compensation – provides medical and wage benefits for employees injured at work. Foreign voluntary workers' compensation extends coverage for employees working abroad, including additional risks and repatriation. Local schemes ensure compliance with local insurance regulations and provide necessary worker protections in specific countries.
- Professional liability insurance – covers businesses against claims for negligence, errors or omissions in the services or advice they provide.
- Directors and officers insurance – protects directors and officers from personal financial losses, legal costs and regulatory investigations.
- Employment practices liability insurance – covers employers against claims related to workplace discrimination, harassment, wrongful termination and employment contract breaches.
- Crime and employee dishonesty insurance – protects businesses from financial losses due to theft, fraud or embezzlement by employees or third parties.
- Cyber insurance – provides coverage for financial losses from data breaches, cyber-attacks and other cyber-related incidents.
- Property insurance – covers damage or loss of physical assets like buildings and equipment due to fire, theft or other risks.
- Political violence and terrorism insurance – insures against losses from politically motivated violence, including war, riots and 'acts of terror'.

Exclusion clauses

It is vital that organisations read the fine print and inquire explicitly about what is and is not covered, thus outlining explicitly the extent of gaps in insurance coverage that they would be liable to cover themselves. Insurance policies may not apply under certain conditions, and the details and interpretation of these exclusion clauses can be crucially important. Organisations can find themselves underinsured and forced to cover unexpected costs on their own.

Insurance coverage may exclude war risks writ large (certain types of war risk or malicious acts, particularly 'acts of terror' such as a bombing in a public place) unless the organisation has a war risk clause as an addition to their insurance agreement or as a separate agreement. Even with a war risk clause in place, insurance companies can exclude specific war zones from coverage. Some of these war zones are pre-determined by the insurance provider. Insurers may also add certain countries to their exclusion clause either upon contract renewal or even during the existing contract by providing written notification (details of this

will be in the contract and most brokers can help organisations with the specific contract language).

Insurance in a country listed under an exclusion clause may not cover injury, illness, death or disability as a direct result of an 'act of war/terror'. This means that a staff death due to a vehicle being hit by an armed drone is not insured, but a staff death due to a road traffic accident is. Premiums to add countries in the exclusion clause to the insurance ('buy back this insurance') can be very high. Should the organisation wish to employ staff in the country regardless, one option could be to 'self-insure', for instance committing to compensate staff working in or travelling to that country to the amount that the insurance company would insure against if the country were not excluded from coverage.

Other examples of exclusions:

- Coverage applies only during work assignments (e.g. in Somalia but not during a period of rest and relaxation in Nairobi).
- Coverage applies only during working hours (e.g. up to 6pm but not afterwards or during weekends).
- Coverage applies only if the organisation has certain written security language, such as the principle of not paying ransoms.
- Coverage excludes staff on short-term contracts, staff from particular countries or volunteers.

It is also important to identify what may be considered a 'pre-existing condition' and therefore not covered – for example mental or physical health conditions. An organisation should discuss their recruitment and due diligence process with their insurance broker/provider.

Insurance considerations

- **Educate staff.** Staff should understand the extent of accident and insurance coverage while working and travelling for the organisation, and the potential impact on any personal insurance they might have (e.g. life insurance policies (such as those taken out with a mortgage) becoming invalid if working in a high-risk area).
- **Coverage at the beginning and end of the employment contract.** Organisations need to know precisely when coverage begins and ends. It is important to determine whether the staff member is covered if they are not yet being paid a salary or have yet to start their assignment, for example.

It should also be clear to both the organisation and the individual at what point after the end of the assignment coverage ceases. This is important for psychological injury, which can manifest long after an incident.

- **Premiums.** Organisations can often negotiate with their broker for lower premiums if they can demonstrate that appropriate risk mitigation measures are in place (e.g. policies, procedures and security training). Some providers offer a credit that can be put towards improving security risk management measures.
- **Equity in coverage.** When discussing insurance policies within international organisations, it is crucial to address the potential disparities and challenges that can arise between national and international staff. These disparities often manifest in access to healthcare and emergency services, such as medical evacuations and the quality of international versus national health services.

Further information

Discussion

Barkwill, D. (2022) *Letter of recommendation: reversing the mental health pandemic amongst aid workers.* AidEx (https://gisf.ngo/resource/letter-of-recommendation-reversing-the-mental-health-pandemic-amongst-aid-workers/).

Reilly, L. (2024) 'Is your mental health covered? Insurance for psychological injury'. Bond (www.bond.org.uk/news/2024/05/is-your-mental-health-covered-insurance-for-psychological-injury/).

Guidance

EISF (2017) *Abduction and kidnap risk management* (https://gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

EISF (2019) *Managing sexual violence against aid workers: prevention, preparedness, response and aftercare* (https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/).

Linnell, H. (2017) *Guide to selecting appropriate crisis management insurance.* EISF (www.gisf.ngo/resource/guide-to-selecting-appropriate-crisis-management-insurance).

World Health Organization, War Trauma Foundation and World Vision International (2011) *Psychological first aid: guide for field workers.* World Health Organization (www.who.int/publications/i/item/9789241548205).

5.5 Health and medical considerations

Because security incidents often involve physical harm to staff, security risk management necessarily involves emergency medical considerations, especially when working in unstable or active conflict settings. Even in the absence of violence, health challenges are inevitable, ranging from exposure to diseases to exacerbation of chronic illness to life-threatening injuries, and require clear mechanisms for prevention, preparedness and response. This chapter outlines the essential elements required for managing medical risks and incidents, including preparedness, first aid and emergency response and medical transfer. The guidance can help organisations identify the measures needed to best respond to medical challenges. However, this chapter is not exhaustive, and organisations are encouraged to consult medical providers to develop policies and protocols most appropriate for their staff and specific contexts.

5.5.1 Prevention and risk mitigation

Many of the medical challenges faced by organisations are preventable. Similarly, the ability to effectively respond to health and medical issues often depends on non-medical considerations, including pre-departure health assessments, robust staff safety and the creation of detailed frameworks for senior staff on how to handle medical incidents.

Swift and appropriate response to health emergencies requires a good understanding of the health and medical risks affecting staff and the surrounding healthcare landscape. This involves including relevant health and medical risks in risk assessment exercises and mapping healthcare resources available to help manage medical emergencies.

A note on occupational health and safety

Occupational health and safety refers to the measures, practices and policies to protect the health, wellbeing and safety of individuals in the workplace as well as the general public. It includes promoting and maintaining the physical and mental wellbeing of workers, preventing work-related illnesses and injuries, and regularly inspecting workplaces for potential hazards.

Occupational health and safety is often codified in government legislation, covering many different measures that are beyond the scope of this GPR. However, this chapter delves into some health considerations most relevant to security risk management, focusing particularly on good practice in preparing for and responding to medical emergencies. For more detailed guidance, consult dedicated occupational health and safety resources, such as the International Organization for Standardization's *ISO 45001:2018: Occupational health and safety management systems* (www.iso.org/iso-45001-occupational-health-and-safety.html).

Assessing local health risks and capacities

Questions to consider before initiating programme activities include general health conditions and trends in the area of operations and the major risks likely to result in medical emergencies. The following are among the most common:

- infectious diseases (e.g. hepatitis, malaria, cholera);
- injuries from armed conflict (e.g. gunshot wounds and injuries from landmines and airstrikes);
- injuries from assaults (e.g. stabbing, beating);
- injuries from road traffic accidents;
- non-communicable illness or chronic health conditions among staff, such as diabetes or hypertension; and
- mental health issues.

Risks will be magnified if there is little or no access to health services in the area, so assessments should include a mapping of available medical resources (e.g. hospitals, ambulances, healthcare providers and medicines or medical supplies) and an assessment of their capacity to support incident response and any specific staff needs. These assessments should also include rapid access to rape crisis centres and other facilities offering specialist care and post-exposure prophylaxis (PEP) for survivors of sexual assault.

► *For more on sexual violence risks, please see Chapter 7.7.*

At a minimum, organisations should have the emergency contact details of reputable local providers as well as the location of the closest tertiary care centres. It is also important to identify providers that are available 24/7 for both physical and psychological care. For mental health support, organisations can consider both locally available and remote services.

▶ *For more details on the mental health risks and support, please see Chapter 5.4.*

It is worth noting that the nearest and/or most reliable health provider may be a medical NGO. It is advisable for senior staff to establish relationships with key health service providers. Doing so can speed up the delivery and improve the quality of care in emergencies.

Medical clearance

If the organisation assigns staff (and any accompanying dependants) to a location away from their home, it has a responsibility to ensure that their health needs can be met there. A medical clearance process reviews fitness for the role (i.e. occupational health assessment) and fitness for undertaking the new assignment (i.e. existing health needs can be met in the country of assignment). Rules around what it is and is not acceptable to ask employees will differ in different legal jurisdictions, and organisations also need to be clear on how this information will be used and by whom. The screening can include a focused review of the individual's medical history (physical and mental health), current treatment plans, medications and risk factors for severe illness or injury. New clearances can be initiated before new assignments, or after significant changes in a staff member's health status or risk conditions at the location. Staff can also be encouraged to update their medical clearance with any change in health status or potential needs while on assignment. This assessment will need to be carried out by qualified professionals and must be treated as confidential (see below).

If a staff member's medical history requires a risk mitigation plan, their physician can work with them to identify an appropriate and feasible plan to propose to the organisation. As part of the process, staff should be made aware of any potential barriers to healthcare access while on assignment, including the potential for delayed or rudimentary care. A general plan can be shared confidentially with country leadership (on a 'need to know' basis) to ensure it can be implemented without undue burden or challenge. Examples include the following:

- A staff member requires a medication that is not available locally. However, the staff member's primary care provider agrees to prescribe a one-year supply for them to use while in the location.
- A staff member's child with a severe allergy to peanuts will be accompanying the family to an international post. The family is trained in the use of an epinephrine auto-injector, and agrees to always travel with two. The family is educated on local diet and how to avoid inadvertent peanut exposure.

As with other safety and security protocols, staff need to be clear that they are expected to comply with all medical and health advice while on assignment, for example including policies requiring vaccination or taking anti-malarial medications.

It is important to ensure that all medical information is submitted either in a confidential document that the organisation will keep secure, directly onto a secure online portal (the organisation's or an external service provider's), or via encrypted email with password-protected files.

Medical confidentiality

It is advisable for each organisation to create guidelines and expectations around medical confidentiality, including whether there may be different protocols depending on the environment and access to medical providers. Staff need to be informed of these measures and have clarity on who has access to their medical information, and the circumstances under which it may be disclosed to others.

Personal medical information must remain strictly confidential except in pre-defined, exceptional circumstances. Providing instruction to relevant staff on medical confidentiality and data privacy is recommended. No one else should have access to the health information of a staff member without their explicit consent.

Staff with responsibility for areas such as health and safety may occasionally need to request additional medical information to support decision-making. In the event of a medical emergency, support staff may extend medical confidentiality to organisational leaders on a limited, need-to-know basis.

Standing capacities and practices

Depending on the assessed risks, mitigation measures may require building or strengthening the capacity of the organisation to respond to medical emergencies and developing the medical components of crisis response and incident management plans.

If health and medical risks are high and the availability of external health resources is low, organisations should consider whether they have the basic capacities to care for their staff in the event of an incident. Not having such capacities would be a failure of duty of care.

Health and medical capacities can include the following:

- **Preventive measures.** Reducing the medical risk in the first place – for example, strong security protocols, coordinating with logistics and supply teams to ensure continued access to necessary supplies.
- **Protocols and procedures.** Creating and regularly re-evaluating protocols for addressing medical incidents, including specific reporting responsibilities and protocols (e.g. medical evacuations, including transport and coordination with local and international evacuation services).
- **First aid capacities.** Providing first aid training (including cardiopulmonary resuscitation (CPR) and any specific needs for remote environments), kits (in all offices (including shared office space), project sites, warehouses, guest houses and vehicles) and guidance (identifying a medical focal point, to be responsible for maintaining kits, including periodic assessments for completeness and expiration dates).
- **Emergency medical supplies and logistics.** Considering what other emergency medical supplies are needed, such as PEP kits, and how to source or access them (whether stockpiling them directly or accessing them through another entity) and ensuring timely replenishment.
- **Health education.** Providing health education, such as webinars/staff briefings on disease outbreaks, and developing a plan for continuous health education on identified risks. This should include mental health risks.
- **Health benefits.** Assessing and optimising the health benefits provided to all staff – both physical and mental – to match staff needs and improve equity (particularly in the case of national aid workers).
- **External medical assistance.** Identifying and contracting external medical assistance vendors to provide physical and mental health information, advice

and referrals, and making arrangements with a provider/clinic for routine/elective care and urgent/emergent medical transport and healthcare access (see Section 5.5.2 below for more details). Establishing and maintaining relationships with local healthcare providers and facilities for support and referrals.

- **Telehealth.** Implementing telehealth solutions – where appropriate and possible – to provide remote consultations with medical professionals, especially in areas with limited access to healthcare facilities.

Health in the workplace checklist

Below are some key elements that organisations can put in place to protect the health of their staff:

- Encouraging regular/annual individual health check-ups
- First aid kits in all offices, residences and vehicles
- First aid training for staff
- Support with accessing medication and contingency arrangements for loss
- Medical clearance for staff deployments and travel
- Medical risk mitigation plans for staff with heightened health risks
- Webinars on relevant/time-bound risks, such as disease outbreaks
- Guidance on medical confidentiality, data privacy and training on handling personal information
- Emergency contacts (for staff and their families)
- Occupational health checks in offices and/or home offices
- Expert ergonomic advice on office equipment
- An accessibility and disability inclusion plan
- Inclusivity and accessibility adjustments to office and other organisational spaces (physical and technological accessibility)
- Telehealth access
- Access to mental health services in general, as well as specialised support following an incident
- Security plans, including health risks and their mitigation

- Written or oral pre-departure health briefings and location-specific health reports (internal or arranged through an external medical assistance provider)
- A suite of resources for staff (in relevant languages), including access to first aid apps, written guidance and contact details, with clear instructions on how to access support in an emergency
- Insurance coverage through a commercial provider or other arrangement in the event of an incident

The greater the risk of a medical emergency (e.g. in active conflict environments or when responding to disease outbreaks), the more an organisation should do to support and train staff, be prepared for incidents and have appropriate and timely response measures in place.

Good practice example: Integrating health during security situations

After the start of violent clashes in Sudan in April 2023, resulting in the collapse of the health system in Khartoum, an organisation arranged telehealth consultations for staff. This included telehealth advice for a staff member's pregnant spouse before and during delivery, and identifying pharmacies with insulin in stock and arranging delivery to a staff member with diabetes.

5.5.2 Preparedness

Medical emergency preparedness

To ensure timely and appropriate responses to medical emergencies and evacuations, it is crucial to focus on medical preparedness before incidents occur. Equally important is encouraging staff to report illnesses or injuries early. For example, an organisation would prefer a staff member to report severe abdominal pain early on, rather than facing a situation where the staff member collapses from a ruptured appendix during transit. Worse outcomes can often

be prevented by staff reporting early and seeking assistance. By ensuring that medical confidentiality is respected, organisations can help improve reporting as staff will likely have more trust in the designated medical lead.

In some circumstances, medical issues can be addressed with support from an external medical assistance provider. An assistance provider is not an insurance company, though some insurance companies may provide (some) medical assistance and evacuation support as part of their package. Providers may be paid by the insurance company (if the assistance provider has a direct billing agreement with them), by the organisation (through a guarantee of payment) or by the staff member.

In the event that staff are hurt or become ill during their work, there needs to be a way of covering related costs. This may be through relevant insurance policies. However, this can be difficult for smaller, local organisations operating on tight budgets and in places with a limited (or no) commercial insurance market. In such cases, organisations could look to self-insurance schemes or support from donors and partners.

▶ *See Chapter 5.4 for more on insurance.*

Support services that security and medical assistance providers can provide include:

- 24/7 access to the closest assistance centre – in an emergency and for everyday advice;
- expert medical, security and travel advice and information;
- location-specific real-time medical and travel security alerts;
- travel checklists; and
- up-to-date contact details in case of an emergency.

With or without external medical assistance, it is good practice for organisations to ensure that there is a point of contact within the organisation for medical questions.

Case example: Restaurant bombing in Islamabad, Pakistan, 2008

In 2008, bombers targeted an Italian restaurant frequented by foreigners in Islamabad, injuring staff from at least two aid organisations. Both organisations had medical assistance providers that identified the same hospital in Islamabad. One organisation had visited the hospital, set up an account and created a relationship. Its staff were triaged to the hospital within the first hour after the attack. The second organisation went to the hospital and asked for its staff to be admitted in accordance with their medical provider procedure. The hospital wanted confirmation of the organisation's capacity to pay. This took several hours to process, and their staff were not admitted to the hospital until after this was completed.

In addition to preparedness for physical health challenges, organisations should also put in place resources and protocols for the provision of mental health support. This requires careful consideration, given the psychological toll of responding in violent environments and the limited access to mental health providers in many contexts.

Mental health needs can take various forms:

- Staff who have ongoing mental health needs that require continuous care and support (e.g. medication and counselling).
- Staff who experience mental health issues such as stress or PTSD as a direct result of work-related experiences.
- Staff whose pre-existing mental health conditions are exacerbated or aggravated by the demands and challenges of their work environment.

Everyone copes with stress – and reacts to shocks – differently. Individuals may demonstrate a range of emotions, from extreme to none at all. Intermittent expressions of emotion are also normal. The psychosocial support provided by professionals, as well as through trained peer support and compassionate leadership, can reduce the likelihood of serious psychological injury, such as PTSD.

What the organisation is able to provide in terms of mental health support should ideally be thoroughly assessed and clearly outlined to staff in advance of an incident, and may vary depending on the affected staff members' needs and wishes.

▶ *See Chapter 5.4 for more guidance on mental health support for staff.*

First aid training

First aid that is delivered in a timely, correct and appropriate manner, with the correct materials, is the single best mitigation measure to reduce the impact of a medical emergency. In remote or resource-limited environments, first aid training should focus on immediate and effective care when professional medical help may not be readily available. This includes trauma-focused first aid training on how to: conduct rapid assessments of injuries/conditions; administer appropriate treatments such as maintaining airway, breathing and circulation (ABCs) and bleeding control; manage pain effectively; and ensure safe patient transport. Understanding the environmental impacts on health is crucial, as factors such as extreme temperatures and altitude sickness can both cause and exacerbate medical conditions and injuries. Additionally, aid workers can be trained on how to use 'resourceful adaptation' – improvising solutions with minimal resources, potentially using natural materials to stabilise and treat the affected person until professional intervention is possible. Specialist first aid training for aid workers (often provided as part of hostile environment awareness training) considers the range (and severity) of medical emergencies (with a particular focus on injuries) that aid staff may face, the limited access to medical services, and the compounding environmental challenges (natural and man-made) that make treatment more difficult.

▶ *See Chapter 5.2 for more information on hostile environment awareness training.*

First aid equipment for remote or resource-constrained environments

In addition to comprehensive training, the availability of appropriate first aid equipment (in appropriate quantities) is essential for effective medical response in remote areas with limited or no access to professional health services. Below is an example list. This is not comprehensive and organisations should seek specialist advice on items to stock and training that is adapted to the context and needs of their staff.

Major medical event response

- **Trauma bandages.** Sterile and absorbent bandages for wound dressing (including chest seals and triangular bandages for slings).
- **Splints.** To immobilise fractures and stabilise injured limbs.
- **Haemostatic agents.** Specialised agents to aid in blood clotting and control bleeding.
- **Tourniquets.** For controlling severe bleeding from limbs.
- **Defibrillator.** In the event of cardiac arrest.
- **Burns dressings gel.** For treating burns.

Wound cleaning and treatment

- **Antiseptic solutions**. For cleaning wounds and preventing infection.
- **Sterile gauze pads.** Used for wound dressing.
- **Adhesive bandages.** To cover minor cuts and abrasions.
- **Antibiotic ointment.** For topical treatment of wounds to prevent infection.
- **Plastic wrap.** For additional temporary wound protection.

Evacuation and transportation

- **Stretchers.** Portable stretchers for carrying injured individuals over rough terrain.
- **Blankets.** To provide warmth and comfort to injured people. Space and foil blankets retain body heat and provide warmth.
- **Portable medical kits.** Compact kits containing essential drugs and supplies.

Personal protective equipment (PPE)

- **Gloves.** Disposable gloves to maintain hygiene and prevent cross-contamination.
- **Face masks.** To protect against airborne pathogens and contaminants.
- **Eye protection.** Safety goggles or glasses to shield against debris and splashes.

Additional supplies

- **Medical tape.** For securing bandages and dressings.
- **Scissors.** Medical-grade scissors for cutting bandages and clothing.
- **Flashlights.** Portable light sources for assessing injuries in low-light conditions.

Ensuring the availability and proper maintenance of first aid supplies is critical to prompt and effective care in challenging environments. Note that more complex treatment, particularly the administration of drugs, must be under the direction of a physician. In emergency situations, this may be provided remotely.

5.5.3 Response to medical emergencies

Aid programming often takes place in areas where access to timely medical care is limited. Rapid response to medical emergencies is critical, as delays in treatment can have severe consequences. This section provides guidance on the skills, equipment and protocols to enable an effective response. All protocols should be developed and elaborated by staff or consultants with medical expertise.

► *The following sections focus on physical medical risks. See Chapter 5.4 for more on psychological risks and good practice.*

Immediate response

While most humanitarian first aid and response protocols focus on traumatic injury (i.e. a severe physical injury that occurs suddenly and requires immediate medical attention), other types of medical emergency may also require immediate response, including cardiac arrest, drowning and heatstroke, for example. Organisations should consider what medical emergencies their

staff need to be prepared to respond to, depending on contextual and staff circumstances. It is good practice for organisations to have plans and protocols in place for managing medical crises, including rapid triage, casualty evacuation and transportation procedures.

Key steps in supporting a person suffering physical trauma or another medical emergency include:

- Ensuring scene safety and using proper PPE before starting any assessment or treatment.
- Quickly assessing and treating immediate threats to life, such as severe bleeding or airway obstruction.
- Deciding if transfer to a higher level of care is required and initiating the transfer process.
- Providing information about the patient's condition to the receiving facility.
- Choosing an appropriate mode of transport based on the patient's needs and available resources.
- Continuing care and monitoring during transport.

The goal is to address critical immediate needs and stabilise the patient so they can be transferred to a medical facility, and to do so within the critical 'golden hour' in the case of a traumatic injury.

Additional considerations for managing major medical events include the following:

- **Emergency communication.** This involves establishing efficient communication to coordinate response efforts and seek assistance, using radios, satellite phones and signalling devices.
- **Medical evacuation (medevac).** Basic navigation and map-reading skills can help facilitate the rapid transportation of patients to medical facilities or evacuation points. It is also good practice for project vehicles to be equipped with basic supplies to enable the transportation of injured or ill staff.
- **Continuous evaluation and improvement of medical incident response protocols.** This might include collecting feedback from response teams to adapt strategies based on lessons learned and evolving challenges.

- **Documentation and reporting.** Documenting and reporting incidents – including near-misses and lessons learned – for incident tracking and analysis and for insurance purposes and any external information needs for medical care and follow-up. Where appropriate, and ensuring confidentiality, this can be linked to an organisation's security incident reporting.

Considerations for aid organisations responding to a mass casualty scenario

Mass casualty scenarios, which can range from hazard-related disasters to large-scale accidents or acts of violence, demand rapid, efficient action and can quickly overwhelm healthcare systems. This can mean considering issues beyond immediate medical care, encompassing aspects of operational management, coordination and ethics.

- **Safety and security.** Ensuring the safety of responders and securing the incident site. Be aware of potential secondary threats or hazards.
- **Rapid assessment and triage.** Quickly assessing the scale of the incident and implementing a triage system to prioritise treatment of victims based on the severity of injuries.
- **Resource management.** Efficiently allocating personnel, supplies and equipment to provide the most benefit. Considering requesting additional resources early.
- **Communication and coordination.** Establishing clear lines of communication between responding organisations, hospitals and command centres. Coordinating efforts to avoid duplication and gaps in response.
- **Public information.** Coordinating consistent and timely communication to the public and media about the incident and response efforts.
- **Documentation.** Implementing systems to track patients, resources used and actions taken for later analysis and potential legal purposes.
- **Cultural sensitivity.** Being aware of – and respectful towards – cultural and religious practices, especially regarding treatment of the deceased.

- **Ethical decision-making.** Being prepared to make difficult ethical choices about allocation of limited resources.
- **Psychosocial support.** In the longer term, providing mental health resources for affected individuals, families and responders.

Aftercare

A well-structured safety and support plan is crucial to the long-term aftercare of aid workers who have experienced a critical medical incident. This plan should prioritise the individual's safety and wellbeing, ensuring they have access to ongoing medical and psychosocial support tailored to their specific needs and wishes (a survivor-centred approach to long-term care is advisable). Long-term medical support can include regular check-ups and access to specialised care as needed, while psychosocial support can include counselling or therapy to address psychological trauma and prevent long-term psychological effects. It is essential to be transparent with affected staff about the extent and duration of support.

Reintegration into work should be carefully managed to support the affected staff member's recovery. This might involve flexible work arrangements, a gradual return to duties or reassignment to less demanding tasks. Maintain regular communication with the individual to assess their comfort and progress, making adjustments as necessary.

► *For more guidance on survivor-centred long-term aftercare for affected staff, see Chapter 5.4.*

Further information

Guidance and resources

American Red Cross (n.d.) First aid training (www.redcross.org/take-a-class/first-aid/first-aid-training).

Center for Substance Abuse Treatment (US) (2014) 'Ch 1: Trauma-informed organizations' in *Trauma-Informed Care in Behavioral Health Services*. Treatment Improvement Protocol (TIP) Series, No. 57 (www.ncbi.nlm.nih.gov/books/NBK207201/).

DeMers, G. and Wightman, J. (2019) 'Mass casualty preparedness and response' in F.G. O'Connor, E.B. Schoomaker and D.C. Smith (eds) *Fundamentals of military medicine*. Borden Institute (https://medcoeckapwstorprd01.blob.core.usgovcloudapi.net/pfw-images/dbimages/Fund%20ch%2034.pdf).

DeNolf, R.L. and Kahwaji, C.I. (2022) *EMS mass casualty management*. StatPearls (www.ncbi.nlm.nih.gov/books/NBK482373/).

International Organization for Standardization (2018) *ISO 45001:2018: Occupational health and safety management systems – requirements with guidance for use* (www.iso.org/iso-45001-occupational-health-and-safety.html).

Rural Health Information Hub (n.d.a) *Emergency preparedness and response for mass casualty incidents* (www.ruralhealthinfo.org/toolkits/emergency-preparedness/4/mass-casualty-incidents).

Rural Health Information Hub (n.d.b) *Partners and collaborators for emergency preparedness and response* (www.ruralhealthinfo.org/toolkits/emergency-preparedness/1/partners-collaborators).

US Centers for Disease Control and Prevention (2024) *CDC Yellow Book: health information for international travel 2024* (www.cdc.gov/yellow-book/index.html).

World Health Organization (2022) *Guide: mass casualty preparedness and response in emergency units*. ReliefWeb (https://reliefweb.int/report/world/guide-mass-casualty-preparedness-and-response-emergency-units).

6 Technology and security

6.1 Managing information and communications security

This chapter focuses on considerations for managing sensitive information and transferring information securely, as well as measures to take when normal methods of communication are disrupted. After an overview of information security, it covers secure communications and the essential elements of a communications plan.

6.1.1 Information security

Information security refers to measures and practices to protect sensitive information from unauthorised access, breaches and misuse. This includes ensuring the confidentiality, integrity and availability of data, particularly in environments where information can be critical to the safety and effectiveness of operations. For humanitarian organisations, this often involves safeguarding personal data, operational details and other sensitive information that, if compromised, could endanger individuals or operations. Information about individual staff, the activities of the organisation, intended aid recipients and contacts can all be used for malign purposes. In some cases, information is not meant to be shared externally. In other instances, information may simply be misconstrued or taken out of context.

Sensitive records for organisations can include:

- Documents on individual personnel such as salaries and performance appraisals.
- Confidential personal information, such as medical records.
- Organisation-specific information (e.g. bank records, legal documents and government agreements).
- Operational assessments (e.g. risk assessments, actor mapping and situation and incident reports, which can be perceived as spying).
- Information on staff movements.
- Records of meetings.
- Information associated with programmes, including aid recipient details.

- Information about finances and cash handling.
- Asset inventories (vehicles, office equipment, radios).

Typical examples of sensitive materials include medical records, identities of staff and aid recipients and operational plans in conflict areas. Mishandling such information can have severe consequences, including risks to personal safety and organisational credibility. Common issues include improper storage of documents, unsecured digital files and lax procedures for disposing of sensitive information. Poor housekeeping can easily result in unauthorised access or accidental data leaks.

In some settings, there is also a high risk of surveillance from state actors, criminal groups or other parties interested in the operations of humanitarian organisations. This can include monitoring of communications, hacking into systems or physical surveillance.

There are several measures that organisations can take to strengthen information security.

- Information security **policies and operating procedures** are crucial for all operational contexts. These documents set out what constitutes 'sensitive information', who is authorised to see it and how it should be stored, communicated, transported, unsensitised or destroyed. Essentially, responsible staff must assess the impact should information be accessed by unauthorised personnel. For example, what would the consequences be if a staff member's personal computer with personal information and images were to be accessed by hostile government actors when arriving in the country?
- **Protocols** can be put in place for data handling, access controls, incident response and contingency planning. These should also address specific challenges, such as managing information in high-risk environments or during emergencies. These protocols can also inform external communications, including media engagement, official statements and social media posts.
- A key way to protect information is to maintain **back-up copies** in multiple locations. This safeguards against loss (but not theft). Both digital and hard-copy backups of vital documents should be kept. Good practices for protecting hard-copy information include proper document handling, secure storage and appropriate destruction methods. In some cases, it may be necessary to quickly destroy sensitive documents (such as shredding

and securely deleting digital files), so minimising on-site documentation is advisable. Restricting access to sensitive information to a limited number of people can provide an additional layer of security.

- **Staff training** is crucial. All staff should be made aware of the importance of information security, how to recognise and handle sensitive information and the specific communications risks of the operational context. This is particularly important for staff with access to sensitive information or those who regularly engage with external actors or manage media interactions, such as communications staff.

Good practice in information security also includes managing communications and digital security and addressing risks emerging from hostile surveillance. Communications security is covered in more depth in the following sections of this chapter, while digital security is discussed in detail in Chapter 6.2. For more information on hostile surveillance, see Chapter 7.5.

6.1.2 Communications planning

The ability to communicate with others is one of the fundamental pillars of security and is especially important in high-risk environments. Security plans and procedures cannot be implemented without the ability to communicate – and, in an emergency, the ability to rapidly communicate with other parties can mean the difference between life and death. As such, a communications plan is just as important to security as a risk assessment, and developing a good communications plan should be taken just as seriously.

A good communications plan is tailored to fit the organisation and meet its specific needs in the context in which it is operating. Communications plans should be customised to each organisation, each office and even each project. Integrating communication security within broader organisational security policies helps ensure a consistent approach across all operations.

Initial considerations

The following considerations should inform the communications plan for any project, office or organisation.

Organisational size and budget

While localised plans may suffice for small organisations, larger entities with multiple offices require comprehensive, compatible strategies to ensure effective inter-office communication and cost efficiency. The goal is to maximise

communication capabilities across the entire organisation. Scalability is crucial; plans should be adaptable to accommodate future growth or contraction, and evolve as the needs of the organisation change.

Budget considerations are crucial. Smaller organisations typically allocate a larger percentage of their overall budget to communications (due to high costs of technology and infrastructure), while larger organisations spend more per staff member but a smaller percentage of the organisation's overall budget. Establishing a realistic budget, both in terms of spending per staff member and percentage of the overall operating budget, is essential. Long-term scalability potentially justifies higher initial investments in sustainable solutions.

Operational context

A separate communications plan may be needed for each operational context. A communications plan that works for an urban, office environment may not be appropriate for a remote rural location, and a communications plan for an urban, office environment in one country may not work in a similar environment in another. Similarly, a communications plan designed for a stationary office may not properly support a mobile team.

The cost and visibility of communications equipment, such as radios and satellite phones, can make them attractive targets for theft or other criminal activities. This risk should be considered as part of communications selection, alongside security measures to mitigate them, such as secure storage, controlled access and regular staff training on the safe use and handling of equipment.

Existing infrastructure

Maximising the use of existing communications infrastructure can increase the options and flexibility of a communications plan, while also minimising cost. However, research must be conducted into the reliability of existing infrastructure as anything outside of the direct control of the organisation can be susceptible to interruption or failure.

- Mobile communications:
  - identify mobile service providers in the area
  - evaluate cell tower coverage
  - determine if mobile-based communication devices should be part of the plan and utilised.

- Internet-based communications:
  - identify local internet service providers
  - assess data speed rates
  - evaluate costs associated with internet services.
- Radio communications:
  - check if an existing radio network is available
  - assess if the organisation needs to build its own infrastructure.
- Electrical infrastructure:
  - evaluate existing electrical systems
  - determine what voltage is available and whether it meets requirements
  - assess the need for back-up power supplies
  - consider if batteries are needed for portable or back-up power
  - if batteries are required, develop a plan for charging and maintaining them.

Communications can be monitored by governments, service providers and other actors. Information security – being careful about who has access to what information and how it is shared – is paramount. It is also an important element in deciding what equipment to use and when.

Case example: Planning for infrastructure disruption

In 2024, Starlink (a private satellite internet service provider) announced it would stop internet services in Sudan, citing a lack of authorisation to operate there. This decision alarmed humanitarian organisations that depended on Starlink for communication amid ongoing conflict and telecommunications outages. They urged Starlink to reconsider, highlighting the service's vital role in coordinating aid and enabling communication for those in need.

Environmental considerations and other types of emergencies

Communications equipment is susceptible to failure in environments with extreme temperatures. Both very hot and very cold conditions require communications equipment designed to withstand extreme temperatures or additional cooling or heating mechanisms. In very humid environments,

a dehumidifying system may be needed. In very rainy environments, extra protection may be needed to protect from water intrusion. Where there is a lot of dirt or dust, devices with fans and moving parts can malfunction if not adequately cleaned and protected.

During emergencies, the volume of calls can surge as people check on loved ones or seek help. This can lead to network congestion, making it difficult to connect calls, whether on landlines or mobile networks. If telecommunications networks are compromised, national emergency alerts may not be delivered effectively, further complicating communication during an emergency.

Office and staff structure

Offices or teams with a smaller staff will generally need less communications equipment than those with a larger staff. Other factors are also relevant. Will staff only work from an office, or will they travel? What mode of transport will they use and will they be travelling in large teams or individually? A small team of five in which each team member travels to a different location daily will need more resources than a team of 20 that only makes a weekly trip to a single location as a group. However, if the team of five were to travel once a week to a particular site, and could each travel to a new site on a different day, then the travel communications resources could be shared, thereby reducing the overall cost. This illustrates how office and staff structure, not simply staff numbers or size, can determine communications needs.

Time considerations

The programme duration is a crucial factor in developing a communications plan. It may not be advisable to invest heavily in fixed communications infrastructure for short-term programming. If the organisation intends to occupy an office location for years, the up-front costs of investing in a robust communications plan make more sense.

Regulatory considerations

It is important to identify what communication equipment is allowed by local authorities. For example, satellite-based communication systems can require special registration and can be banned in some jurisdictions. While humanitarian organisations may be able to apply for an exemption, especially if working or partnering with the UN, approval is not guaranteed and must be sought before importing communication devices into the country. Knowing which communication equipment is legal can prevent costly mistakes.

Case example: Choosing the right equipment

It is also important to consider which communication equipment is normally used in certain contexts and by whom. In 2023, a humanitarian organisation operating in eastern Ukraine was inadvertently targeted by the Russian military. An after-action review revealed that the humanitarian organisation was mistaken for a Ukrainian military target because it had a Starlink satellite dish on the roof of its building. The only other Starlink systems in the area were being operated by Ukrainian military units.

Interagency coordination

In many high-risk operational areas, telecommunications services may be provided by the Emergency Telecommunications Cluster (ETC). The ETC is a global network that collaborates with various organisations to deliver shared communication services during humanitarian emergencies. This includes offering voice communication options and other essential services to humanitarian organisations, national authorities and affected communities, particularly where existing communication infrastructure may be compromised or unavailable. The local ETC working group, or the World Food Programme (WFP) as the lead agency of the ETC, can provide information on what services are available in the area of operations. Risks to ETC services are similar to those of other telecommunications, including infrastructure and disruption vulnerabilities. In some regions, there may be opportunities for organisations to take part in the UN Radio System, or specific frequencies may have been designated for NGOs.

Intended communication partners

The next step in creating a communications plan is to consider the people and organisations that need to communicate with each other. Each of these groups will likely require a separate communications plan, but not necessarily separate communications equipment.

Internal communications

Internal communication is most straightforward as the organisation has complete control over equipment, methods and policies. Internal communications are also the easiest to fix when problems arise. Internal communications can be the

most expensive, as the organisation must cover all costs related to equipment purchases, maintenance and training.

When creating an internal communications plan, the organisation must first consider who and which groups need to be in communication with each other. If several individuals on a small team are travelling to an in-country location separately, a communications plan can be developed to address how each team member will communicate with the others. A second communications plan might outline how that team communicates with other teams, while a third might detail how those teams communicate with their head office. A separate communications plan could map out how each individual or group communicates with relevant internal stakeholders.

External communications

External communications encompass all interactions with individuals or groups outside the organisation. This can include aid recipients, local community representatives, partner organisations, government entities, funding agencies and UN agencies. It is advisable for communications plans to be developed for each entity. In some contexts, humanitarian organisations may be required to adopt the communications plan or equipment being used by the external entity. This is not always the case, but before developing a communications plan identifying who the external stakeholders are and what systems they use can save the organisation time and money in the long run.

▶ *See Chapter 4.4 for more information on communications during a crisis.*

Emergency communications

An emergency communications plan needs to outline multiple methods for individuals and teams to contact emergency services, both within the country and within the organisation. Not all countries and contexts have standardised national telephone numbers for emergency services – and provision should be made in case telephone networks go down.

The organisation will usually need to adopt the communication methods, plans and protocols outlined by emergency service providers, and so understanding these protocols before developing an organisational emergency communications plan is beneficial.

6.1.3 Communications equipment

This section outlines the basic types of communications equipment that an organisation might consider in its planning.

Types of equipment

High frequency radios

Operating at frequencies between 3 and 30 megahertz (MHz), high frequency (HF) radios (e.g. portable, vehicle or base station equipment) are typically used by amateur radio operators, military personnel and humanitarian organisations, including the UN. Humanitarian organisations have come to rely on HF radios less and less as mobile and satellite technologies have become more ubiquitous and less expensive.

The main advantage of these radio systems is that they bounce communication signals off the upper atmosphere, which allows for longer-range transmissions. HF radios are thus capable of communicating with each other hundreds of kilometres apart. The primary disadvantages of HF radio communications are that atmospheric disturbances can disrupt the signal (e.g. weather and sunlight). HF radio systems also generally require a high level of expertise to set up, maintain and operate, which can entail investment in training (for example in handling the equipment and using codified language: communications that are unencrypted can be intercepted by anyone with a radio operating on the same settings and frequency). These radios also typically require a large antenna, which can increase the vehicle's visibility, potentially making it a target for hostile actors, theft or mistaken identity as a military asset.

Table 11 Security considerations for HF radio communications equipment

Type	Advantages	Disadvantages/vulnerabilities
Vehicle radio	• Powered by the vehicle (radio is on when the vehicle is on) • Can communicate longer distances • Accessible to everyone in the vehicle	• Signal quality can depend on the vehicle's location • Requires a generally high knowledge level to be able to troubleshoot issues • Maintenance needs can be higher due to driving conditions • High initial costs • Must be working on both ends for communication • May require a licence to operate

Type	Advantages	Disadvantages/vulnerabilities
Portable radio	• Smaller than a vehicle radio • Portable – not tied to vehicle power • Can be used with no existing infrastructure	• Requires a high level of knowledge to set up and use properly • Requires batteries, which can run out • Equipment is heavy • High initial cost • Must be working on both ends for communication • May require a licence to operate
Radio base station	• Uses existing power (wall outlet or generator) • Can communicate very long distances • Accessible to everyone • Not dependent on any existing infrastructure other than power	• Requires a very high level of knowledge to set up and maintain • Must be working on both ends for any communication to go through • High initial cost • May require a licence to operate

Very high and ultra high frequency radios

Very high frequency (VHF) radios operate on the 30 to 300 MHz band, and ultra high frequency (UHF) radios operate between 300 MHz and 3 gigahertz (GHz). These radios are used by a wide range of people, from the military, police and other emergency services to hobbyists.

The main advantage of VHF and UHF radios is instant communication in a simple-to-use package that is relatively cost-effective. The main disadvantage is that VHF and UHF radios generally require line-of-sight, and so communication can be difficult in urban areas with tall buildings, for example, or in mountainous regions where the terrain obstructs the direct path between radios.

While the maximum distance of VHF and UHF radio communication varies by manufacturer, power, antenna and other factors, portable VHF and UHF radios must be within a few hundred metres to a few kilometres from each other or they will not be able to communicate. UHF radios generally work better in urban environments as the frequency band is better able to penetrate walls and other objects than VHF radios. VHF radios are generally better suited for longer-range outdoor communication. VHF and UHF radios are a poor choice for over-the-horizon communication unless repeaters are used.

Like HF radios, VHF and UHF radios operate on a point-to-point basis, meaning that one radio directly communicates with another without needing an intermediary to relay the transmission. However, repeaters can be used as intermediaries, accepting the transmission from one radio and retransmitting it to extend the signal's range. Like HF radios, signals travel long distances and, if unencrypted, are susceptible to interception by anyone with a radio operating on the same settings and frequency. Also similar to HF radios, these systems require expertise to set up, maintain and operate.

Table 12 Security considerations for VHF and UHF radio communications equipment

Type	Advantages	Disadvantages/ vulnerabilities
Vehicle radio	• Powered by the vehicle (radio is on when the vehicle is on) • Can communicate over several kilometres • Accessible to everyone in the vehicle	• A good signal will require the vehicle to be within range of the intended receiver • Requires some knowledge to set up (though not to use) • Maintenance needs can be higher due to driving conditions • Must be working on both ends for communication • May require a licence to operate
Portable radio	• Smaller than a vehicle radio • Portable – not tied to vehicle power • Can be used with no existing infrastructure	• Requires batteries, which can run out • Limited range (circa 8 kilometres or less, depending on conditions) without a repeater • Must be working on both ends for communication • May require a licence to operate
Radio base station	• Uses existing power (wall outlet or generator) • Can communicate over longer distances than portable radios • Accessible to everyone • Not dependent on existing infrastructure other than power	• Requires a moderate level of knowledge to set up and maintain • Must be working on both ends for any communication to go through • May require a licence to operate

Type	Advantages	Disadvantages/ vulnerabilities
Repeater	• Extends the communication range by rebroadcasting the radio transmission • Requires power but no other existing infrastructure • Does not require anyone to operate it once set up	• Can be expensive • Must have power and a building space to set up • May require many repeaters to establish a large communications network • Requires a moderate level of knowledge to set up and maintain but not to operate • May require a licence to operate

Mobile devices

Mobile devices require an existing mobile network that repeats the transmission from one mobile device to another along the network or, depending on the situation, through the internet. The main advantages of mobile devices are the ubiquity of the equipment, relatively low cost, widespread existing infrastructure and ease of use. The main disadvantages are reliance on existing infrastructure (without mobile coverage devices cannot communicate) and the fact that mobile companies act as intermediaries in the communications chain, allowing them to intercept and potentially monitor communications. Many governments have the power to either shut off mobile communication or heavily monitor activity. Many also require mandatory SIM-card registration, which typically involves providing personal details, including a valid ID, to activate the card. Finally, while a lot of data and voice communication is encrypted, preventing the majority of users from intercepting the communication and eavesdropping, it is not always possible to keep communications secure from the mobile provider or the government.

Table 13 Security considerations for mobile communications equipment

Type	Advantages	Disadvantages/vulnerabilities
Mobile phone (voice)	• Equipment is low-cost and universally used • Training needs are minimal • Lower mobile signal strength is needed for voice versus data communication	• Must have mobile network coverage and an active plan • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors • Higher risk of network congestion during emergencies
Mobile phone (data)	• Equipment is low-cost and universally used • Training needs are minimal • Information flow and data rate can be very high, allowing large amounts of data to be communicated in a short time	• Must have mobile network coverage and an active plan • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors
Mobile hotspot	• Equipment costs are low • Multiple devices can communicate through one hotspot • Some hotspots can use multiple mobile networks, allowing for greater coverage	• Must have mobile network coverage and an active plan • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors

Type	Advantages	Disadvantages/vulnerabilities
Smart device	• The device itself connects directly to the mobile network without the need for another device as an intermediary • Devices can range in size (from very small to very large) • Devices can come with existing equipment (smart display installed in a vehicle, for example)	• Must have mobile network coverage and an active plan • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors • Communication options are almost always limited to the device's installed software options

Hardline devices

Hardline devices connect to each other through an existing network of cables (underground, above ground, undersea). The major advantage of hardline devices is that they can generally communicate large amounts of voice or data reliably and at speed. They can also be more reliable than mobile devices because the hardline connection needs to be broken for service to be interrupted, while mobile devices rely on the signal strength from a remote connection to a cellular tower. A weakness of hardline connections is that the connections themselves cannot be moved and are therefore not portable. Further, the existing infrastructure of hard-line connections is not as ubiquitous as cellular towers, and disruption can take longer to repair.

Table 14 Security considerations for hard-line communications equipment

Type	Advantages	Disadvantages/vulnerabilities
Landline phone	• Harder to intercept than mobile phone voice calls • Easy to use • Traditional landline phones, particularly analogue models, do not require an external power source to operate	• Completely unencrypted • Diminishing availability • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors

Type	Advantages	Disadvantages/vulnerabilities
Dial-up	• Provides internet access	• Only available in some more remote locations • Relies on existing phone lines • Very slow data rate • Can be disrupted by natural hazards or other environmental factors
Digital subscriber line (DSL)	• Faster than dial-up • Low cost • Widely available • Can use wifi routers so multiple devices can communicate on one line	• Relies on existing phone lines • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors
Cable	• Very fast data transfer rates • More reliable than DSL • Connection can slow during peak usage times • Can use wifi routers so multiple devices can communicate on one line	• Relies on existing cable lines (originally run for cable television) • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors
Fibre	• Very fast data transfer rates • Most reliable connection • Can be expensive • Less prone to outages or slowdowns • Can use wifi routers so multiple devices can communicate on one line	• Relies on fibre optic lines • Can be subject to government monitoring • Can be shut down by governments at any time • Can be disrupted by natural hazards or other environmental factors

Satellite communication devices

Satellite communication devices communicate via a network of satellites (or a satellite constellation) rather than cellular towers. The advantage to this is that one satellite can provide coverage to a much larger ground area than a cellular tower. Satellite communication devices are also more difficult to disrupt and governments generally do not have the ability to shut off services as they can with mobile devices or other terrestrial networks.

The two main disadvantages to satellite devices are that the antenna of the device must have a direct line-of-sight to the open sky (so they cannot be used from inside a building unless an antenna is placed outside) and devices and services are more expensive than with mobile communications. It is also important to recognise that they are not entirely immune to government control or other forms of interference (including targeted disruption). Some governments prohibit satellite communication devices altogether, some place restrictions on certain carriers and others require all satellite devices to be registered. Finally, a major risk of satellite communications is the dependence on satellite service providers, which may choose to abruptly end services. While this is a challenge for all communication services, it is more pronounced in satellite communications due to the limited number of operators.

Table 15 Security considerations for satellite communications equipment

Type	Advantages	Disadvantages/vulnerabilities
Satellite phone	• Almost universal coverage • Can call any phone	• Some providers have better coverage than others • Service can be expensive • Phone must have a direct line of sight to the sky • Can be illegal in some jurisdictions, or require a licence/authorisation
Satellite push-to-talk device	• Almost universal coverage • The signal can be more reliable than with a satellite phone • Can talk with multiple people at once (like a radio system)	• Some providers have better coverage than others • Service can be expensive • Device must have a direct line of sight to the sky • Can be illegal in some jurisdictions or require a licence/authorisation • Takes a moderate level of knowledge to set up

Type	Advantages	Disadvantages/vulnerabilities
Emergency locator/ beacon	• Almost universal coverage • Signal can be more reliable than with a satellite phone or push-to-talk device • Can be fully encrypted • Microburst transmission does not require an ongoing, active signal	• Some providers have better coverage than others • Device must have a direct line of sight to the sky • Can be illegal in some jurisdictions or require a licence/ authorisation • Generally limited to small data amounts (text messages, small files, a single picture) or just location information • Messages can be slow to send or receive
Satellite internet	• Rapidly expanding coverage • Full internet access • Can connect multiple devices to one connection	• Some providers have better coverage than others • Service can be expensive • Device must have a direct line of sight to the sky • Can be illegal in some jurisdictions, or require a licence/authorisation • Can take a moderate level of knowledge to set up

6.1.4 Choosing equipment and creating a plan

Once a basic understanding of the types of communications equipment and the organisation's communications needs are identified, it is time to start building a communications plan.

Choosing secure equipment

Security staff are often asked which communication methods and equipment are the most secure. The answer depends on location, circumstances and timing, as technology changes quickly. Good practice recommends thorough risk assessments to select communication tools that suit the operational needs and context, alongside redundancy to safeguard against communication failures.

Organisations can also consider encryption options when selecting communications equipment. Encryption can be used on most communications equipment, including radio systems, hardline devices and satellite communications. Encryption can significantly enhance the security of

communications but will require compatible equipment or software. The use of encrypted communications may be subject to regulations.

It is advisable for organisations using encryption protocols to regularly update and audit these to address new threats and vulnerabilities. Adopting a layered security approach, combining encryption with other measures like access controls and secure user authentication, provides a more robust defence against potential security breaches. It may be appropriate to use codes when communicating sensitive information. This is discussed briefly in the sections below.

Creating a communications plan: introducing required redundancy

Communication plans should incorporate redundancy, meaning they should ensure that communication remains functional even if one component fails. A Primary, Alternate, Contingency, and Emergency (PACE) plan is designed to maximise communication redundancy and thereby reduce risk. The PACE plan outlines the sequence in which different communication methods are to be used. For instance, mobile phones might be designated as the primary method of communication. If this method fails, the team then switches to the alternate (e.g. VHF radio), followed by the contingency method (e.g. satellite communication) if that also fails.

There are two key principles with a PACE plan. First, PACE refers to types of communication, not the devices themselves. For example, two devices that both rely on mobile networks cannot serve as the Primary and Alternate methods in a PACE plan because a disruption to the mobile network would render both inoperable. The only exception is radio communication since radio systems do not rely on an intermediary: two complete VHF or HF radio systems can serve as separate communication methods within a PACE plan. However, each system must be entirely independent. If there is a single point of failure, such as a shared radio base station at an office location, then these do not count as separate systems.

The second principle is that a PACE plan is sequentially applied – each step is only used if the previous method fails, ensuring a structured and reliable communication process. For example, if the primary method of communication is a mobile phone, it should be the first choice in any situation. An emergency does not automatically necessitate switching to the 'Emergency' option of the PACE plan. The team only moves to the Alternate method when the Primary fails, and similarly only moves to the Contingency method when the Alternate fails, and so on.

Below are some examples of PACE plans. Note that each section of the PACE plan has a different type of communication, even if multiple devices are used to communicate within that type.

Table 16 Example PACE plan (primary office location)

P/A/C/E	Type	Device	Primary use(s)
P	Hardline	• Cable internet via commercial provider to whole-building wifi coverage	• Data communication • Internet access • Voice communication
A	Mobile	• Mobile back-up to cable internet connection • Mobile phone • Mobile hotspot	• Voice communication • Data communication • Internet access
C	Satellite	• Back-up satellite internet connection to select wifi points and select staff	• Data communication • Internet access
E	VHF radio	• Radio base station	• Emergency voice communication

Table 17 Example PACE plan (remote but fixed site)

P/A/C/E	Type	Device	Primary use(s)
P	Satellite	• Satellite internet connection to whole-building wifi • Satellite phone	• Data communication • Internet access • Voice communication
A	HF radio	• Radio base station • Vehicle radios	• Voice communication
C	VHF radio	• Radio base station • Portable radios	• Voice communication
E	Mobile	• Mobile phone	• Emergency voice communication that requires a 20-minute drive to an area with mobile coverage

Table 18 Example PACE plan (mobile team)

P/A/C/E	Type	Device	Primary use(s)
P	Mobile	• Mobile phone • Mobile hotspot	• Voice communication • Data communication • Internet access
A	VHF radio	• Vehicle radios • Portable radios	• Voice communication
C	Satellite	• Satellite phone • Emergency locator	• Voice communication • Emergency notification
E	None	• N/A	• N/A

A PACE plan reduces risk but can never eliminate it. There are situations and locations where it can be impractical or impossible to have four separate types of communication in a PACE plan (see Table 18 with the last example PACE plan). Where this occurs, risk can be further reduced by increasing the devices within a particular communication type as this provides as much back-up as possible to a single point of failure.

A note on app-based communications

It is increasingly common to use third-party apps to send text messages and make voice or video calls. These app-based communications tools are widespread and easy to use. However, apps cannot fill a separate space in a PACE plan because they are dependent on the hardware on which they are installed. Thus, a mobile phone will only occupy one space on the PACE plan even if it has three different communication apps installed. *For further discussion on app-based communications, see Chapter 6.2 – Security in a digital world.*

Staff training

After a PACE plan has been developed, a training plan can be created to ensure that all staff members understand when to use which forms of communication, and that they are proficient in the use of each device. The training plan will usually depend on the types of communication and the devices used. While very few staff members will likely need to be trained on how to use a mobile phone, most staff will require instruction on how to use certain software or other applications on the phone. In contrast, very few (if any) staff members will likely be immediately proficient in setting up and running an HF radio system. It is good practice to ensure that all staff are trained to use and regularly practice using all forms of communication in the PACE plan.

Issues to consider in developing training include identifying who is going to conduct the training; what budget (time and money) is required for staff to become proficient in the use of all of the equipment; and what level of technological knowledge is required for which users. Some communications equipment is so complicated that it may require one or several full-time staff to set up and maintain.

Initial training on communications equipment can be part of the onboarding process, followed by regular refresher training. Spot training can help identify weaknesses and get staff used to implementing the PACE plan. For example, a security staff member at one international organisation would turn off the wifi when visiting a country office to test how the staff responded.

It is also helpful to ensure that staff are trained in secure communication practices, including recognising threats and properly handling sensitive information. Regular practice opportunities allow staff to refresh their skills, including how to turn on the equipment, use it, maintain or troubleshoot basic problems and ensure the equipment is charged and stored properly.

Equipment maintenance

All communications equipment is subject to failure over time and will, at some point, need to be replaced. This is an important consideration when developing a communications plan. Manufacturers should be able to provide an estimated replacement timeframe (that is, the expected period of time a particular device will need to be replaced). Organisations should try to plan for the replacement of all devices in order to estimate long-term budget needs and pre-empt communication disruptions.

In addition to the equipment itself, common maintenance items that need to be budgeted for include replacement batteries, battery chargers, antennas or other peripheral items, phone cases or screen protectors, and any other accessories necessary for the safe operation of the equipment.

Case example: The importance of maintenance

For cost reasons one organisation decided not to use satellite as its primary means of communication, opting instead to reserve it as back-up for emergencies. An audit of its satellite phone infrastructure found that approximately 40% of the batteries were dead, and 40% of the phones needed a software upgrade.

All communications equipment, regardless of its place in the PACE plan, should be regularly tested. Tests should be conducted at least once a week on communications equipment that is not regularly used, and daily on communications equipment that is used daily. In addition to routine testing, devices should ideally be tested before any planned travel and before staff arrive at a new location. For example, if a team is going out on a site visit, every device on the PACE plan can be tested to ensure it is working before the team leaves and retested on arrival. This does not need to be overly burdensome, but a simple text message or test call to ensure connectivity is advisable. In addition to the equipment itself, it is advisable that batteries and other peripheral equipment are also regularly tested.

Protecting communications equipment

Communications equipment comes with different operating parameters and protection needs. Any electronic equipment that is plugged into an electrical socket needs to have protection against power outages and voltage or amperage surges. In a hot environment equipment will usually need to have a mechanism to keep devices cool, while devices operating in a very cold environment may have to be kept warm. One of the greatest challenges for communications equipment in vehicles is to keep the devices clean and free of dust. Protection requirements should be budgeted and planned for.

▶ *For more information on precautions against theft, see Chapter 7.2 – Site security.*

► *For more information on precautions against communication interception or digital intrusion, see Chapter 6.2 – Security in a digital world.*

6.1.5 Good practice in communication methods

Clear and secure communication

The key principles of operational discipline in communications are clarity, brevity, timeliness and relevance. It is imperative that staff are aware of and trained on the risks of communicating certain types of information, especially when using unencrypted methods.

Radio operating procedures

Clarity and brevity in radio communications are achieved through the use of procedure words (or 'prowords') and communication signals (such as 'over' or 'say again'). Clarity is enhanced when:

- messages are prepared in advance;
- messages are presented point by point;
- users stop talking when they have nothing to add;
- users speak in short sentences, in plain language and standard 'broadcasting' language, rather than local dialects; and
- users do not speak too quickly, especially when the recipient needs to write the message down, and they speak in a normal tone of voice (shouting can impair the quality of reception).

There is an internationally agreed radio protocol for emergencies (with many local variations). The caller seeks clearance on the channel by repeating three times 'MAYDAY MAYDAY MAYDAY' or 'PAN PAN PAN', usually followed by 'ALL STATIONS'. There is an absolute obligation to accept emergency calls and to interrupt ongoing conversations. A security message that does not indicate a threat to life or property (e.g. notice of civil disturbances in a town that, therefore, needs to be avoided) can be initiated by repeating 'SECURITY, SECURITY, SECURITY'.

Emergency communication procedures

Emergency communication procedures should be established early and routinely practised by all staff members. The box below provides guidance on the essential information to be communicated in an emergency – regardless of the mechanism of communication. Practising this sequence can help reduce errors in the event of an emergency.

How to communicate in an emergency

State the information in the format and sequence below:

1. Who you are.
2. Your organisation.
3. Your location (e.g. GPS location, or nearest major routes or towns).
4. Type of emergency (e.g. mine accident, under fire or medical evacuation).
5. Number of people injured.
6. Current negative activity – is it safe for a rescue now?
7. Past negative activity.
8. Next time of communication.
9. How to contact the caller (e.g. phone number or radio frequency).
10. Other information.

► *For more guidance on reporting incidents, see Chapter 4.4.*

It is also important that staff members regularly confirm all emergency contacts and procedures so that everyone is able to contact the appropriate personnel in the event of an emergency. This can be done through monthly check-in calls, for example.

During times of crisis, decision-makers can be bombarded with so much information that it is impossible to differentiate fact from rumour. To be effective, it is important to minimise communications to only those matters of direct importance. Again, this can be achieved through training and discipline.

Communicating sensitive information

When communicating sensitive information, staff should consider the following factors:

- **Assess the need for communication.** Before sharing sensitive information, evaluate whether it is necessary to disclose the information and whom it should be shared with. Ensure that sharing is justified and appropriate.

- **Verify recipient authorisation.** Confirm that all recipients are authorised to receive the information. This helps prevent unauthorised access and ensures compliance with privacy regulations.
- **Limit information sharing.** Share only the minimum necessary information required for the purpose of the communication. Avoid providing extraneous details that could increase the risk of exposure. All those with access to the information should understand and respect confidentiality.
- **Choose appropriate communication channels.** Select the most secure and appropriate method of communication. For sensitive information, consider private face-to-face meetings or secure messaging platforms instead of unencrypted communications equipment or public forums.
- **Document communications carefully.** Keep accurate records of communications involving sensitive information, noting who was informed and what was discussed. This can help in maintaining accountability and transparency.
- **Manage consent.** If the information relates to a particular individual or their circumstances, it is good practice to obtain their consent to share their personal information and be transparent about who may have access to the information and for what purposes.

Staff can be made aware that, even under the best circumstances, communications can be accessed, and they must be mindful of what is being communicated. In high-risk settings, it is sensible to encourage staff to express themselves in a moderate, factual and non-partisan way – and where staff might be targeted, encoding certain information that could give away staff positions or movements, for example using code words to designate offices, people, routes and route points, vehicles and types of cargo. This is popular but seldom well managed and, therefore, not very effective. It requires careful briefing and agreements in advance. Ideally, the code words or phrases are known by heart (rather than written down in a codebook) and changed regularly. For politically sensitive events, metaphorical expressions can allow for plausible denial. A code that is broken can constitute a major vulnerability. Too many code words may confuse staff.

Further information

Guidance and resources

Davis, J. et al. (2020) 'Module 9, Communications and information security' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/).

EISF (2010) *The information management challenge: a briefing on information security for humanitarian non-governmental organisations in the field* (https://gisf.ngo/resource/the-information-management-challenge/).

Emergency Telecommunications Cluster (n.d.) *Services & activities* (www.etcluster.org/services-activities).

GISF (n.d.) *Communications technology hub* (https://gisf.ngo/communications-technology-and-humanitarian-delivery/).

WFP (n.d.) Emergency Telecommunications Cluster (www.wfp.org/emergency-telecommunications-cluster).

6.2 Security in a digital world

This chapter discusses digital risks and their real-life consequences for aid workers. It provides an overview of potential mitigation measures as well as the growing challenges presented by harmful information, such as misinformation, disinformation, malinformation and hate speech.

6.2.1 Digital security

Global connectivity technologies are enabling greater outreach, aid delivery and operational stability, as well as enabling affected populations to share their experiences and perspectives. Developments in mobile technologies, notably 4G and 5G, have brought faster data transmission and expanded bandwidth capacities, while next-generation satellite equipment, such as Starlink, has vastly expanded the potential for working online in highly remote locations, offering reliable, fast and affordable internet access.

These evolutions in technology also carry increased risk for aid organisations, their staff and operations, and the populations they serve. The increasing volume and severity of cyber-attacks and other digital threats (such as hacking, surveillance, online abuse and data leaks) mean that every individual user must be equipped to safeguard themselves, their devices, their communications and their data against digital threats. Establishing comprehensive digital security practices is increasingly important for humanitarian organisations.

Digital security

Digital security, for the purposes of this chapter, refers to the protection and safeguarding of aid workers who use or are affected by digital tools and technologies. This includes informational harm as well as 'cybersecurity' – the technical aspects of the security of the computers, mobile devices, applications, data and connectivity services aid workers rely on.

Digital threats to humanitarian organisations are widespread and multifaceted. Mobile device security, use of untrusted and potentially hostile networks and internet sources, interception of data and digital communications, and the physical security of devices and data all require attention. The digital sphere also presents intelligence-gathering opportunities for potentially unfriendly or hostile entities. While digital security often falls under IT, security staff are increasingly involved in digital security discussions, as digital threats can have significant physical security implications for aid workers. For instance, hacking or unauthorised access to sensitive data, such as travel itineraries or personal information, can lead to targeted physical attacks, kidnapping and harassment by hostile actors. Cyber-espionage and surveillance can allow state and non-state actors to monitor the movements and communications of aid workers, making them vulnerable to interception or ambush.

The spread of misinformation or disinformation through digital channels can also incite hostility or violence from local communities or armed groups, directly endangering staff. The theft of devices containing critical data can lead to breaches that compromise the security of operations, putting both aid workers and local communities at risk. Thus, the intersection of digital and physical security is critical, with lapses in digital security potentially leading to grave real-world consequences. Security staff need to understand the types of digital threats aid workers may face and how they can work with other organisational teams to mitigate digital risks, including promoting digital hygiene practices among staff.

6.2.2 Digital threats and cybersecurity risks

The nature of digital threats can vary depending on the level of the target, which can be an individual, a specific organisation or the aid sector overall. While there is often overlap (e.g. individuals may become victims when their organisations are targeted), it is beneficial for organisations to discuss the specific risks and implement measures to mitigate threats across all three levels. This may be particularly helpful in regard to the risks of harmful information.

Threat actors

Digital threats can emanate from a range of actors with different motives (for instance economic, ideological or strategic). Examples include the following:

- **Cybercriminals.** Cybercriminals – individuals, small groups, gangs or large criminal organisations and enterprises – are primarily driven by the desire for financial gain and seek targets of opportunity. Some also have ideological or political motives.

- **State actors.** Humanitarian organisations operating in conflict zones or areas of high political tension can find themselves in danger of accidental or intentional targeting by governments and foreign state actors. Government entities operating in the digital sphere are typically driven by national security and other political concerns and can be highly capable of executing successful cyber-attacks and conducting digital surveillance, as well as harmful online influencing campaigns.
- **Non-state armed actors.** As digital resources become increasingly accessible, their potential use by non-state armed actors increases. These groups may use the same tactics as cybercriminals for financial gain, as well as gathering intelligence and weaponising information for ideological and political reasons. They may use online influencing campaigns, disinformation and other targeted attacks to undermine an organisation's operations or perceptions among local communities.
- **Others.** Disgruntled employees, or people with a grudge against the organisation or specific staff members, can pose threats in the digital sphere, just as they can offline. Social media influencers with political agendas can use their platforms to spread harmful information about aid organisations or the aid sector as a whole. Threats may also emanate from the public influenced by these influencers or online campaigns.

Types of digital threats

The following is a list of some of the digital security challenges aid workers can face. These can overlap or take place concurrently – all have the potential to translate into physical security risks.

Table 19 Types of digital threats

Threat	Description
Harassment and online hate speech	Online harassment and threats, including hate speech, often directed at aid workers from marginalised groups or with public-facing roles. This can include targeted campaigns spreading inflammatory or derogatory content aimed at inciting violence or undermining the credibility and safety of individual aid workers, a particular organisation or the aid community as a whole.
Identity theft	Theft of personal information.
Social engineering	Manipulation of individuals into divulging confidential information, often through seemingly innocuous interactions.

Threat	Description
Misinformation, disinformation and malinformation	The spread of harmful information about aid organisations, their staff or their work, undermining credibility, trust and operational effectiveness. This can include online campaigns or data leaks that damage the reputation of the organisation or individual aid workers. While this harmful information can be deliberately engineered, it can also spread organically on social media platforms.
Phishing and email scams	Designed to steal credentials, introduce malware or gain unauthorised access to sensitive information. These risks have spread to mobile devices in the form of 'smishing' (phishing via SMS text messages). Scams enhanced by artificial intelligence (AI) such as 'vishing' attacks (phishing via voice call, in which AI is used to clone the voice of a person known to the target) are also on the rise.
Online scams and fraud	Financial scams targeting organisations and individual aid workers, often through deceptive online practices.
Hacking and system intrusions	These aim to access or disrupt organisational systems, often seeking to steal sensitive data or cause operational damage.
Data theft	Theft of sensitive organisational data, including information about aid recipients, financial records and confidential communications.
Ransomware and malware attacks	Introduction of malware, including ransomware, to lock down systems or data until a ransom is paid or to damage systems outright.
Cyber espionage and surveillance	Monitoring and surveillance by state or non-state actors, especially in regions where aid organisation activities are viewed with suspicion, might include: the interception of communications and information about aid distribution locations; the tracking of movements or geolocation of staff or aid recipients; or identification of staff, potentially culminating in further cyber-attacks or even physical harm. There have been documented incidents of state actors using spyware against organisations. *For more details on hostile surveillance and related mitigation measures, see Chapter 7.5.*

6.2.3 Online targeting of individual staff

Online attacks – particularly through social media and other platforms – can result in the direct harassment, abuse, intimidation and blackmail of aid workers.

Direct targeting is a growing and serious threat, particularly for those in public-facing roles or from under-represented or marginalised groups (e.g. women and individuals who identify as LGBTQI+).[86] Harassment can take various forms, including cyberstalking, doxing (where private information is published online without consent) and malicious impersonation. Cyberstalking may involve persistent and threatening messages, while doxing can expose sensitive personal information to the public (such as home addresses and family details). Malicious impersonation, where attackers create fake profiles to mislead or tarnish the reputation of the victim, can severely damage both personal and professional relationships and credibility.

Case example: Online harassment in the Middle East

A blog in Jordan posted profile pictures from gay dating apps, resulting in severe public backlash and potential danger for the individuals whose photos were published, who faced immediate and significant risks, including social ostracisation, harassment and potential legal repercussions. This incident highlights the importance of digital security and the potential consequences of digital exposure in hostile environments. It also underscores the need for aid organisations to provide clear guidance to staff on protecting their online identities, and the importance of monitoring local online spaces for potential threats, and taking proactive measures to mitigate risks.

Source: Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response.* GISF (https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/).

Online attacks can have profound psychological effects on their targets, leading to stress, anxiety and a pervasive sense of vulnerability. The impact can be even more severe when personal information is weaponised in environments hostile to certain identities or affiliations, or where aid workers already face significant risks due to the nature of their work.

86 For more detailed examples of the digital risks faced by LGBTQI+ aid workers, see Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response.* GISF (https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/).

These direct attacks are also more difficult for organisations to have visibility over, and attackers may even be colleagues of the victim. The entire process of a digital threat – identifying the target, finding vulnerabilities, contacting the victim, delivering the threat, reaching a resolution – can take place entirely online, making it hard to detect by anyone who is not directly affected.

To mitigate these risks, organisations can provide comprehensive digital security training that covers safe online behaviours, how to recognise and respond to online risks (such as harassment and exploitation) and how to manage digital identities and footprints. Aid workers can be encouraged to use secure accounts, enable strong privacy settings on social media and consider the use of pseudonyms to protect their identities. It is also advisable for organisations to have robust policies in place to address digital exploitation, offering clear guidelines on how to handle incidents of harassment and safe spaces for affected staff to raise concerns or report incidents.

Support services should be available to those affected, including mental health resources to help workers cope with the psychological impact of being targeted, as well as legal assistance to address any potential breaches of privacy or security. By creating a strong support network and fostering a culture of digital security awareness, organisations can help protect their staff from the increasing threat of online attacks and their potentially severe consequences.

▶ *See Chapter 5.4 for more on staff care, including mental health support.*

Responding to a direct online attack

The following are steps an organisation might consider following an online attack on an individual.

- **Identify the aggressor**. Identify the attacker and their actions, if possible.
- **Assess breached platforms.** Identify compromised platforms or devices, and reset passwords. Change usernames and credentials if necessary.
- **Contain unwanted information.** Contact social media or telecommunications providers to contain the spread of unwanted content. Ensure secure communication when doing so.

- **Alert financial institutions.** Notify, if advisable, banks or financial institutions if there are monetary demands or threats.
- **Protect organisational integrity.** Minimise the impact on the organisation to avoid endangering other staff or damaging the organisation's reputation.
- **Notify relevant authorities.** Depending on the situation, alert any relevant authorities, for example local police or the embassy (if a foreign national was affected).
- **Communicate with staff.** Inform staff to report any further threats directly to security and other responsible personnel.
- **Consider evacuation or relocation.** If the situation escalates into a physical threat, consider evacuating or relocating affected individuals.
- **Limit information disclosure.** Share only information necessary to contain the threat, avoiding the disclosure of sensitive details.
- **Document the incident.** Keep detailed records of all communications, threats and actions taken. This can be helpful for legal purposes and future protection.
- **Provide psychosocial support.** Offer counselling or other psychosocial support for affected staff.
- **Engage in counter-messaging.** If misinformation or harassment is public, consider a controlled, official response to counter false narratives and maintain credibility.
- **Review and strengthen security protocols.** Once the incident has been resolved, review and update digital security protocols to prevent future occurrences.
- **Ongoing monitoring.** Continue monitoring the victim's online presence and related platforms for further threats or harassment.

6.2.4 Harmful information

Harmful information (misinformation, disinformation, malinformation and hate speech) is rapidly becoming a serious threat to aid organisations. With the rise

of social media, AI-generated pictures and videos, and the increasing number of alternative information-sharing websites, this type of threat will only increase in frequency, scope and severity.

Information shared in humanitarian crisis settings can become harmful through several different mechanisms – described in more detail below – and can involve a wide range of external actors with different intentions, targets and means of disseminating information. Trust and faith in institutions, authorities and traditional sources of information is diminished, leaving space for alternative sources of information, including social media. Although alternative platforms can amplify otherwise unheard voices, they can also allow harmful information to go unchecked and have unprecedented reach across audiences, including stakeholders in humanitarian action.

It is important to be mindful that sources of harmful information can be actors that aid organisations do not usually engage with, such as tech companies, the private sector, social media platforms, influencers and general users.

Key definitions

Misinformation refers to inaccurate or false information that is shared without the intent to deceive. It often results from misunderstandings, errors or a lack of proper verification, rather than a deliberate attempt to mislead. This is distinct from disinformation, which is information that is deliberately false or misleading. Malinformation refers to true information that is taken out of its original context or manipulated in a way to mislead or cause damage. Hate speech is content that targets a group or individual based on their inherent characteristics, such as ethnicity, religion or gender.[87]

Security impact

Humanitarian organisations often prioritise acceptance as their core security risk management approach, rooted in a principled response that adheres to neutrality, independence, humanity and impartiality. Harmful information is particularly dangerous as it can erode perceptions of a principled response among stakeholders, often independently of any action taken by the organisation or its staff. Such information can also be used to manipulate public perception, shaping narratives and undermining the credibility of humanitarian organisations. Examples include the following:

87 For a detailed discussion of definitions, see Wardle, C. (2024) *A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation.* Department of Peace Operations (United Nations) (https://peacekeeping.un.org/en/new-report-finds-understanding-differences-harmful-information-is-critical-to-combatting-it).

- **Propagating false narratives.** Actors may spread false narratives to discredit humanitarian organisations, portraying them as biased or politically motivated, even as cover for espionage. This sows distrust, undermines public support and justifies restrictions on access to crisis areas. Even true information about aid efforts can be manipulated. After the 2023 earthquakes in Türkiye, a story about the Turkish Red Crescent selling tents was spread and amplified on social media, fuelling criticism of the government's disaster response. This manipulation undermined public trust in both the government and the Turkish Red Crescent.[88]
- **Accusations of misconduct.** Disinformation campaigns might falsely accuse aid workers of crimes or misconduct, such as corruption or collaboration with enemy forces, damaging reputations and potentially leading to legal or operational repercussions, even expulsion. Aid organisations may themselves be charged with spreading misinformation or disinformation.
- **Spreading false information.** Disinformation, such as fake information about distributions or other interventions shared online, can cause confusion, disrupt operations and damage the trust between organisations and communities. False information exploiting cultural or religious sensitivities, such as rumours about vaccination campaigns, can incite violence against aid workers and disrupt critical operations. Disinformation can also create false perceptions of bias in aid distributions.
- **Discrediting humanitarian reports.** State actors may use misinformation to undermine the credibility of reports documenting human rights abuses or crises, often labelling them as 'fake' to dismiss their findings. For instance, Myanmar has denied the existence of the humanitarian crisis affecting the Rohingya people.
- **Impersonation.** Actors may hack the communications of humanitarian organisations to spread false information directly.
- **Weaponisation of information.** Hostile actors may hack into data systems to alter records or leak sensitive information, undermining the organisation's credibility or targeting specific groups. In 2022, a hack exposed the data of over 515,000 vulnerable people, endangering them and damaging trust in the ICRC.[89]

88 Insecurity Insight (2023) *The role of social media in the spreading of the Turkish Red Crescent Tent Sale Story in Türkiye*. Social Media Monitoring (https://insecurityinsight.org/wp-content/uploads/2023/08/The-Spreading-of-the-Turkish-Red-Crescent-Tent-Sale-Story.pdf).

89 ICRC (2022) *Cyber attack on ICRC: what we know* (www.icrc.org/en/document/cyber-attack-icrc-what-we-know).

- **Incitement of violence and hate speech.** Social media posts can be used to incite violence or other negative behaviours towards humanitarian personnel, locations, assets and operations. Hate speech, which targets groups based on identity, presents real and immediate concerns.

Case example: Disinformation examples in Ukraine

Disinformation affects everything from personal security and the reputation of individual aid organisations to the overall perception of the aid sector and its ability to achieve humanitarian goals and implement programmes.

During the conflict in Ukraine, Russian-affiliated actors employed disinformation to obstruct and manipulate humanitarian operations. One significant instance involved the dissemination of false information about evacuation routes. Pro-Russian Telegram channels falsely claimed that the Ukrainian military was blocking certain evacuation routes or that these routes were under attack. This caused confusion and fear among civilians, leading them to avoid using safe evacuation routes or delay their departure from dangerous areas.

The ICRC also faced a significant disinformation campaign targeting its humanitarian efforts in Ukraine when Russian-affiliated actors spread false narratives, including claims that the organisation was involved in forced evacuations of Ukrainians to Russia and setting up offices in southern Russia to filter Ukrainians. The baseless accusations, which were disseminated across social media and occasionally appeared in mainstream media, aimed to discredit the ICRC's work among Ukrainians and jeopardise its operations.

Sources: Center for Civilians in Conflict (2023) *When words become weapons: the unprecedented risks to civilians from the spread of disinformation in Ukraine* (https://civiliansinconflict.org/publications/research/when-words-become-weapons-the-unprecedented-risks-to-civilians-from-the-spread-of-disinformation-in-ukraine); ICRC (2022) *Ukraine: addressing misinformation about ICRC's activities* (www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities).

Risk assessment of harmful information

In addition to ensuring that digital threats, including harmful information, are incorporated into existing risk assessment processes, organisations should equip responsible personnel, such as social media staff, with the tools needed to consider harmful information risks directly.

▶ *See Chapter 4.1 for more on risk assessments.*

An example of a risk assessment process for potentially harmful information is below, adapted from the Médecins sans Frontières Mis/Disinfo Assessment tool.[90]

- **Understand the target.** Who is the target (individual, programme, organisation, sector) and how are they being targeted?
- **Understand the purpose.** Is the harmful information being shared with the intent to harm, or is information becoming harmful organically through misinterpretation and widespread sharing?
- **Understand the source.** Is the information being driven by a particular source (e.g. a group or influencer)? Is this wholly new information or has it been shared before?
- **Classify.** Is this content low or high risk? (See Table 20.)
- **Evaluate.** What kind of risk does this pose? (See Table 21.)

Table 20 Classification of content risk

Low	Medium	High	Urgent
Harmless misunderstanding/ mistaken information	Misinformation that could cause harm	Deliberate harmful information involving the organisation or its staff	Targeted propaganda against the organisation or its staff

90 See GISF (2023) *Online risk to real-life harm: disinformation and social listening workshop resources* (www.gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

Table 21 Evaluation of content risk

	Low	Medium	High	Urgent
Gravity	No risk of real-life harm or threat	Moderate risk of harm	Indirect risk of real-life harm	Direct threat of real-life harm
Scale	Not much attention	Moderate pickup, some comments	Significant attention in short time	Going viral
Target	No specific target	Indirectly impacts the organisation and its staff	Directly impacts the organisation and its staff	Directly targets the organisation and its staff
Source	Source with limited reach	Localised movement, ad hoc	Coordinated, purposeful	Networks with significant reach

Mitigation measures

Once risks of harmful information have been assessed, there are several possible mitigation measures, listed below. These must be carefully evaluated and tailored to specific risks, as what works well in one instance may worsen the situation in another.

- **Evaluate the information landscape.** Understand where and how target communities obtain their information by identifying trusted sources and communication channels. This helps target and counter harmful narratives before they spread widely.[91] Organisations should ensure that actor mapping and analysis includes individuals or groups that can influence the spread of harmful information.
- **Develop and implement communications strategies.** Design robust communications strategies that include monitoring social media for both positive and negative content relevant to the organisation, its work and the aid sector as a whole. Create a strong social media presence on contextually relevant platforms, regularly updating them with positive, honest and transparent content that highlights core messages and humanitarian

91 To this end, an information ecosystem assessment can be helpful. See, for example, Internews (2015) *Mapping information ecosystems to support resilience* (https://internews.org/wp-content/uploads/legacy/resources/Internews_Mapping_Information_Ecosystems_2015.pdf).

principles. 'Verified', for example, is an initiative launched by the United Nations in collaboration with Purpose to combat misinformation related to Covid-19.

- **Monitor harmful content and changes in perceptions.** Invest in social media 'listening' initiatives to track sentiment over time and flag negative content before it turns into a real-life security threat.[92] Organisations can also use public resources that track and analyse content to help identify potential threats, harmful information and public perceptions that could affect the security and effectiveness of aid efforts.[93]
- **Sensitise and train staff.** Provide digital literacy training to staff, focusing on how to handle spurious content and manage their online footprint. Encourage staff to act as the organisation's eyes and ears online, reporting potential risks.
- **Build strong networks.** Develop strong networks with partners both within and outside the humanitarian context for mutual support and information verification. Pre-existing relationships can mitigate reputational risks and allow the swift sharing of counter-messaging. Establishing relationships with local media outlets and radio stations can also be an effective way of sharing accurate information about humanitarian activities in the area.
- **Raise awareness.** Partner with other organisations, policymakers and media to raise awareness about harmful content and pressure social media companies to act responsibly.
- **Establish clear roles and responsibilities and collaboration across teams.** Ensure that roles and responsibilities are clear with regard to monitoring and documenting information that is harmful or has the potential to cause harm, that staff are adequately trained and supported, and that there are clear protocols for when and how relevant information will be shared with other parts of the organisation, including security staff.

In general, it is advisable for organisations to have a strategy in place to effectively respond to incidents of harmful information. Response actions may include the following:

- **Reporting harmful content.** Use the social media platform's reporting tools to flag harmful content and engage directly with social media companies to expedite the review and removal process.

92 Iacucci, A. (2023) *Social Listening*. Slide deck. GISF (https://gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

93 For example, Insecurity Insight (n.d.) *Social media monitoring* (https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring).

- **Engaging in fact-checking and counter-messaging.** Consider collaborating with fact-checking entities to verify information, and develop counter-messages to correct false narratives. Effective counter-messaging involves understanding the main nodes and links through which the information spread originally, and targeting those same networks. This can help maintain trust and credibility while preventing the spread of misinformation. However, in some cases it may be better not to draw further attention to the false information.
- **Rebuilding trust after harmful information campaigns.** Focus on rebuilding trust with affected communities through transparent communication and engagement. This can include demonstrating how the organisation protects data it collects relating to targeted populations and other local actors, and that it has considered the potential harms and risks if it were to fall into the wrong hands.
- **Collaborating with authorities.** If content poses an immediate threat, consider notifying law enforcement or relevant authorities.

Responding to incitement of violence on social media

Incitement to violence on social media is prohibited by most platforms, including Meta (Facebook and Instagram), which has community standards against such content. If an organisation encounters posts that incite violence, it can use the platform's reporting tools or directly contact the company to flag the content as violating community standards or that could lead to potential harm, prompting a review and potential removal. Providing detailed information should help expedite the review process. If the content poses an immediate threat, law enforcement or relevant authorities should be notified, as and when appropriate, to ensure a prompt response.

Follow-up activities may include:

- Flagging content that may become harmful in the future for continuous monitoring.

- Recording the steps taken and the outcomes following an incident to inform future risk assessments, risk mitigation and response measures.
- Carrying out an after-action review to identify lessons to improve future efforts, as would be done for a critical security incident.

6.2.5 Digital communications technologies and their risks

Many risks come from the use of untrusted networks – which usually means any network that is not under the organisation's control. Any network with an unknown level of security can be considered inherently insecure. The following section presents an example list of risks associated with digital communication technologies. It is not meant to be comprehensive, but rather provides information regarding common areas of concern.

Mobile networks

Mobile networks have inherent security flaws, including susceptibility to unauthorised access and data interception, particularly where regulatory oversight is lax or compromised.

A major risk of using mobile networks is the potential for hostile parties to intercept data streams. These parties could be local governments, gangs, criminal organisations or states with access to the carrier networks. This interception could lead to leakage of sensitive communications or operational data, such as staff locations and operational movements.

Public wifi

Public wifi sources, such as free or paid wifi at airports, cafes and hotels, are a common and often necessary means of internet connectivity for travelling staff. The primary attack vector is man-in-the-middle (MITM) attacks, in which a malicious third party eavesdrops on the network, intercepting or interfering with communications.

There is no way of knowing whether a wifi network operator has securely configured a network – and the risk of a successful MITM attack increases where this is not the case.

There is also the risk of a malicious actor setting up an 'evil twin' – a fake wifi network that uses the same name as a legitimate wifi source, causing users to connect to the fake network unintentionally. The attacker will then be able to intercept all internet traffic on this fake wifi network. By default, phones and

devices may automatically connect to 'known' wifi networks, meaning an attacker could set up this same network in an airport and dozens or even hundreds of devices could passively connect to it.

Local internet service providers

Local internet service providers (ISPs) can provide a faster and more stable internet connection for long-term or permanent office locations as well as short-term project locations. It is still advisable to use caution with these connections and take steps to secure them.

While the ISPs themselves are likely not significant threats, any system or device connected to the internet is at risk of attack. ISPs could be infiltrated by cybercriminals or state actors, leading to the potential interception of sensitive communications and data. Having additional layers of encryption can increase protection.

AI-related risks

AI tools present opportunities and challenges for aid organisations. For aid workers, challenges include the potential for data breaches and the propagation of biased or inaccurate content. Hostile actors can use AI to amplify misinformation, conduct phishing attacks or even deploy AI-driven surveillance to monitor and target aid workers. These risks underscore the need for caution and strict adherence to security protocols when interacting with AI, both in terms of using AI tools and protecting against AI-driven threats from hostile actors. There is also growing concern about the use of AI systems in military targeting, including the risk of misidentification and the potential for erroneous strikes. Organisations such as the ICRC are drawing attention to this risk.[i]

[i] Viveros Álvarez, J.S. (2024) 'The risks and inefficacies of AI systems in military targeting support' *Humanitarian Law & Policy*, ICRC (https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/).

Public charging stations

Public charging stations, such as at airports, train stations and hotels, include standard electrical wall outlets and USB charging ports. Heightened risk is linked specifically to the USB charging ports.

'Juice jacking' is where a compromised USB charging port contains a small device that can send commands to a phone, tablet or other device plugged in for charging purposes. This could potentially be used to install malware or allow an attacker remote access. Where it is not possible to access an electrical wall outlet to charge a device, a USB data blocker can be plugged into the USB charge port before use to protect against a potential juice jacking attack.

6.2.6 Security controls and digital hygiene

Organisational mitigation measures

Technology needs assessment

In order to understand the threats that an organisation and its staff may face – and in order to implement appropriate risk mitigation measures – it is important to identify what technology may be used by staff to carry out their work, and the different risks of different types of projects. This involves understanding the programme's scope and the digital activities of all stakeholders. This technology needs assessment would cover equipment and communication devices as well as software and apps.

Organisations will usually have less control of and visibility over devices that are for personal use – although these can be equally at risk. Organisations can manage the risks associated with personal devices by providing training for staff on good digital hygiene practices (no matter what device is used), setting protocols around using personal devices for work-related purposes, and restricting access to sensitive information on personal devices.

Risk assessments

When it comes to effectively assessing risks, a collaborative, cross-team approach is beneficial. IT teams can focus on evaluating potential threats in hardware, software and systems, while managers can review the software their teams use to identify vulnerabilities. Communications staff can perform a 'digital context analysis' to understand how various stakeholders might use digital media, and security staff can identify security vulnerabilities and link these to broader physical threats stemming from digital exposure. Programme staff can

assess the risks of abuse, criminal targeting or manipulation related to digital aspects of their programmes, such as cash transfers, advocacy or data collection. It is crucial to recognise that, like physical threats, digital threats do not affect everyone equally. Any risk assessment will need to be inclusive and consider how different identity profiles can affect digital risks.

Organisations also need to remember that there is overlap in the digital security of staff, the organisation and relevant communities. A breach in one area will have repercussions for others, and any risk assessment and mitigation measures should consider their interdependence.[94]

Aid workers can also become collateral damage in a digital attack targeting a third party that holds their organisation's data or whose services the organisation uses – this is something that also needs to be factored into any risk assessment. Finally, organisations are responsible for complying with relevant data protection regulations (such as the European Union's General Data Protection Regulation (GDPR)).

▶ *See Chapter 4.1 for more on risk assessments.*

Repeatable security protocols

Protocols help users conduct themselves and carry out operations in a consistently secure manner. Keeping protocols simple and repeatable — meaning they are standardised, well documented and can be easily followed in the same way each time — helps ensure they are consistently adhered to. Protocols can include procedures for requesting and acquiring devices, reporting lost or stolen devices, acquiring internet connectivity and good practice for user behaviour.

VPN and web security

Virtual private network (VPN) and web security tools protect end-user devices, data and communications while on the move and using untrusted networks. A VPN encrypts data as it leaves a user's device so that it remains protected and masked from hostile actors as it crosses untrusted wifi networks, mobile networks and the internet. Web security generally comes in the form of web content filtering, and is a critical first line of defence against malware, malicious websites, phishing attacks and other online threats. Combined with a VPN tool that encrypts internet traffic, this can provide significant protection and shielding for end users and their data.

94 To learn more, see Davis, J. et al. (2020) 'Module 4, Digital security' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/).

Using SSL-encrypted websites that display the 'padlock' is a good idea when on unsecured wifi. Many government websites, especially in the countries where most aid work takes place, have been compromised in the past and are not configured to have encryption. Caution needs to be exercised.

Enterprise security solutions provide advanced, comprehensive and organisation-wide security features to protect an organisation's data and users, even across remote or unsecured networks. These tools include 'zero trust', 'SSE (secure service edge)', and 'SASE (secure access service edge)'. Enterprise solutions go beyond individual website encryption by offering a broader security framework to protect an entire organisation's digital ecosystem.

App-based communication tools

When weighing the risks and benefits of different apps and platforms for communication, there are three things to consider.

- **What is the security of the app?** Open-source apps hosted in countries with robust privacy protection laws and good security practices will be more secure than proprietary apps hosted in countries where the government controls the network and privacy laws are ignored or unenforced.
- **Who owns the data from the app?** Is the data stored only on the device itself? Is the data stored in the servers of a private company, government or non-profit? It is important to know where the data is located and what path it takes in order to properly assess the security of a particular app.
- **What is currently available or in use in the countries of operation?** A highly secure app may be a poor option if it is unavailable for download in a particular country, if it cannot be installed on the devices used by the majority of staff or if it is unfamiliar or difficult to use.

Mobile device management

A mobile device management (MDM) platform monitors and protects mobile devices. An MDM allows for centralised remote management of devices, including the ability to wipe sensitive data from devices that are lost or stolen. If this is not possible, encrypting the devices and using strong passwords and private folders is a good measure.

Physical device security

Physical security as an important aspect of keeping people, devices and data safe. If hostile actors can get their hands on a device, they can likely compromise it. The risk of data leaks is reduced considerably if files are encrypted and devices are password-protected and never left unattended. Reporting a lost or stolen device as soon as possible to the IT and security teams allows for rapid response to mitigate the potential impact. There may be cases where staff are required to temporarily surrender devices to authorities for inspection. If there are any suspicions of tampering, or if the device leaves the sight of the staff member for any period, IT and security will want to know.

Although not always practical, Faraday travel bags can protect mobile devices from potential attacks while travelling. Electromagnetic waves – such as those used for wifi and mobile communications – are prevented from entering the bag, which can block unwanted connection attempts or mobile device surveillance.

Digital hygiene practices

Digital hygiene refers to standard practices to maintain digital security and mitigate digital risks. Digital hygiene can help to maintain a consistent digital security baseline by promoting good, repeatable behaviours and protocols. Below are some suggestions for sound security hygiene practices, which can be part of an organisation's security protocols and training.[95]

Use strong passwords and multifactor authentication

- **Create strong passwords.** Staff can create strong, complex passwords using a mix of characters and regularly update them, avoiding reusing the same passwords across multiple accounts. A good practice is to use 'three random words' for easy-to-remember yet secure passwords.
- **Use multifactor authentication.** Multifactor authentication provides an additional layer of protection against stolen or cracked passwords.

Install device and app updates

- **Keep everything updated.** Ensure all operating systems and installed apps are updated before travelling. If available, a mobile device management system can be used to keep devices and apps up to date automatically.

95 For more guidance, see ACT Alliance (2019) *Basic cyber security. A guide for all to manage digital security* (https://gisf.ngo/wp-content/uploads/2021/10/ACT_Digital_Security_Guidelines_2019.pdf).

Harden devices

- **Secure device settings.** Devices typically do not ship in their most secure state, so organisations should establish device hardening standards as part of their security policies. Staff can implement device hardening by configuring secure device passcodes, disabling unnecessary apps and services, enabling device encryption, turning on lockdown modes and disabling wireless radios when not needed.

Minimise app and social media usage

- **Limit app usage.** Each installed app is a potential vulnerability. It is advisable to minimise unnecessary app usage, especially while travelling, and consider removing apps that are not needed.
- **Use secure communication apps.** End-to-end encrypted communication apps are preferable but a robust assessment can be conducted to determine the safest app for use in different contexts.
- **Social media precautions.** Avoid social media posting while travelling, as this can leak information. Turn off location services and review privacy and sharing settings on all apps.
- **Photo metadata.** Turn off location settings when taking photos and remove metadata from images before sharing them.

Strengthen email security

- **Be cautious with emails.** Avoid clicking on links or opening attachments from unknown sources. Verify the sender's email address, especially when dealing with sensitive information.

Manage and encrypt data

- **Encrypt sensitive data.** Ensure all sensitive files are encrypted before storing or sharing them. Anonymise personally identifiable information.
- **Secure file sharing.** Use secure methods for sharing files, such as encrypted email services or secure file-sharing platforms.
- **Back up data.** Regularly back up important data to secure, encrypted storage to prevent loss.
- **'Clean as you work'.** Consider data use when moving between locations: data such as photos which is safe to use and share in one location may pose security risks if seen in another. To mitigate these risks, send necessary photos by secure electronic means, then promptly remove them from the device.

- **Delete data.** Securely delete data when no longer needed.
- **Review and control access.** Regularly validate data accuracy, control access and maintain audit trails to ensure only authorised personnel can access critical data. Staff should be especially careful about what kind of data they collect, how they store it and who has access to it. Security staff may collect and have access to very sensitive personal information on staff and other actors, and need to be mindful of the risk of information being used to harm the organisation, its staff, the people it is trying to help or its operations – even if this is shared with legitimate interests, such as state actors.[96]

Use the internet securely

- **Use VPNs on public wifi.** Always use a VPN when accessing the internet over public wifi networks.
- **Avoid unsecured websites.** Recognise and avoid websites that are not secured with HTTPS (a secure protocol designed to send data between a web browser and website).

Report incidents

- **Follow established reporting protocols.** Report suspected digital security incidents, such as phishing attempts or potential data breaches.

Organisations should consider developing training sessions and seminars to improve digital literacy and cover good digital hygiene practices for staff for both organisational and personal technology, including social media. Regular refreshers and updates on emerging digital threats are crucial to ensure that aid workers remain vigilant and well-prepared to safeguard themselves and their colleagues in the digital space.

Further information

Digital security guidance and tools

Access Now (2020) *Digital security helpline: Self-doxing guide* (https://gisf.ngo/resource/access-now-digital-security-helpline-self-doxing-guide/).

ACT Alliance (2019) *Basic cyber security. A guide for all to manage digital security* (https://gisf.ngo/wp-content/uploads/2021/10/ACT_Digital_Security_Guidelines_2019.pdf).

96 As exemplified by the sharing of personal information from ethnic Rohingya refugees by UNHCR with the Bangladeshi government, which in turn shared the information with authorities in Myanmar. See Human Rights Watch (2021) *UN shared Rohingya data without informed consent* (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent)

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

Front Line Defenders (n.d.) Security in-a-box (https://securityinabox.org/en/).

GISF (2021) 'Module 2: Information management' in *Keeping up with COVID-19: essential guidance for NGO security risk managers* (https://gisfprod.wpengine.com/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers-module-a2-information-management/).

GISF (n.d.a) Resources & background materials (DCS). *Digital cyber security.* (www.gisf.ngo/themes/digital-cyber-security/resource-background-materials-dcs/).

GISF (n.d.b) *2. Digital security.* NGO Security Toolbox (www.gisf.ngo/toolbox-pwa/resource/2-digital-security/).

GISF (n.d.c) *Digital security resources. Communications technology and humanitarian delivery* (/www.gisf.ngo/themes/communications-technology-and-humanitarian-delivery/digital-security-resources/).

Tactical Tech (n.d.) *Holistic security manual* (https://holistic-security.tacticaltech.org/index.html).

Research and discussion on digital security

Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

GISF (2023a) *The intersection of technology and human security*. Podcast. Evolving NGO security risk management (www.gisf.ngo/resource/evolving-ngo-security-risk-management-ep4-the-intersection-of-technology-and-human-security-gisf-podcast/).

GISF (2023b) *Humanitarian security in an age of uncertainty: the intersection of digital and physical risks* (www.gisf.ngo/resource/humanitarian-security-in-an-age-of-uncertainty-the-intersection-of-digital-and-physical-risks/).

Human Rights Watch (2021) 'UN shared Rohingya data without informed consent' 15 June (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent).

ICRC (2022) 'Cyber attack on ICRC: what we know'. 24 June (www.icrc.org/en/document/cyber-attack-icrc-what-we-know).

Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response*. EISF (https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/).

Rodenhäuser, T., Staehelin, B. and Marelli, M. (2022) 'Safeguarding humanitarian organizations from digital threat' *Humanitarian Law & Policy*, ICRC (https://blogs.icrc.org/law-and-policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/).

Viveros Álvarez, J.S. (2024) 'The risks and inefficacies of AI systems in military targeting support' *Humanitarian Law & Policy*, ICRC (https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/).

Resources on harmful information

Blake, J. (2020) *Disinformation and security risk management for NGOs*. GISF (www.gisf.ngo/blogs/disinformation-and-security-risk-management-for-ngos/).

Center for Civilians in Conflict (CIVIC) (2023) *When words become weapons: the unprecedented risks to civilians from the spread of disinformation in Ukraine* (https://civiliansinconflict.org/publications/research/when-words-become-weapons-the-unprecedented-risks-to-civilians-from-the-spread-of-disinformation-in-ukraine/).

GISF (2023c) *Online risk to real-life harm: disinformation and social listening workshop resources* (www.gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

Insecurity Insight (2023) 'The role of social media in the spreading of the Turkish Red Crescent Tent Sale Story in Türkiye' *Social Media Monitoring* (https://insecurityinsight.org/wp-content/uploads/2023/08/The-Spreading-of-the-Turkish-Red-Crescent-Tent-Sale-Story.pdf).

ICRC (2021) *Harmful information – misinformation, disinformation and hate speech in armed conflict and other situations of violence: ICRC initial findings and perspectives on adapting protection approaches* (https://shop.icrc.org/harmful-information-misinformation-disinformation-and-hate-speech-in-armed-conflict-and-other-situations-of-violence-icrc-initial-findings-and-perspectives-on-adapting-protection-approaches-pdf-en.html).

ICRC (2022) *Ukraine: addressing misinformation about ICRC's activities* (https://www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities).

ICRC (2023) *How misinformation and disinformation harm ICRC's humanitarian work in Burkina Faso* (www.icrc.org/en/document/burkina-faso-how-misinformation-disinformation-harm-humanitarian-action).

Insecurity Insight (n.d.) Social media monitoring (https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring).

Internews (2015) *Mapping information ecosystems to support resilience* (https://internews.org/wp-content/uploads/legacy/resources/Internews_Mapping_Information_Ecosystems_2015.pdf).

Tiller, S., Devidal, P. and van Solinge, D. (2023) *The fog of war and information.* MSF Analysis (https://analysis.ocb.msf.org/the-fog-of-war-and-information/).

Wardle, C. (2024) *A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation*. Department of Peace Operations (United Nations) (https://peacekeeping.un.org/en/new-report-finds-understanding-differences-harmful-information-is-critical-to-combatting-it).

7 Managing specific threats and risk situations

7.1 Travel security

Aid workers often face heightened risks while travelling. This makes effective travel risk management crucial, not only for maintaining access to critical areas but also for ensuring the safety, security and confidence of travellers. Managing these risks is a shared responsibility between the organisation and its staff, and requires comprehensive policies, thorough training and robust contingency plans. By maintaining a strong focus on safety and security, humanitarian organisations can continue to travel to even the most challenging environments to carry out their work. This chapter discusses general travel security considerations and outlines good practices for various modes of travel.

7.1.1 General considerations

Travel risk management policy

A well-defined travel risk management policy serves as the foundation for all security practices related to travel, transforming potential chaos into structured preparedness.

A comprehensive travel risk management policy typically includes the following:

- **Consistent standards and procedures.** A travel risk management policy sets out clear and consistent standards and procedures for both the organisation and the individual. This can include identifying potential risks, establishing protocols for mitigating the risks, and outlining procedures for emergency response. The clarity provided by such policies fosters a unified approach to travel risk management, enabling organisations to identify and mitigate risks before they materialise.
- **Centralised vs. decentralised management.** Organisations should carefully consider which aspects of travel risk management are best handled centrally and which are best managed at a local level. This decision can be based on the resources available and the specific risks associated with each travel scenario. For instance, while airline safety data might be managed centrally, the selection of appropriate airlines and travel routes may be better handled at a local office by staff familiar with local conditions.
- **Traveller rights and personal risk thresholds.** Traveller rights can be clearly defined in the policy, particularly in relation to personal risk thresholds. It is good practice for staff to be informed of their right to withdraw from

missions or travel if they believe the risks are too high. This not only protects the individual but also ensures that travel is carried out by those who are fully prepared and confident in their ability to manage the risks.

▶ *See Chapter 1.1 for more on personal risk thresholds.*

- **Pre-travel security briefings.** Security briefings prepare travellers for their journeys by providing essential information, including the itinerary and other details of the trip, context-specific and personal risks, appropriate responses to these risks, and recommendations on necessary documentation and items to bring. Briefings usually also cover organisational guidelines, pertinent internal policies, emergency contacts and information on travel insurance and assistance services. These briefings can be delivered through various methods, including documents, videos or discussions with security focal points, and should be adapted to the specific type of travel and the traveller's personal risk profile.
- **Training.** The organisation's requirements for travel, including mandatory training, should be clearly outlined in travel policies, employee contracts and security plans. Organisations should ensure that training and briefings are not given exclusively to international travellers, but are also available to resident staff who may be travelling to different areas within a country.

▶ *See Chapter 5.2 for more on training.*

Establishing a comprehensive travel risk management policy creates a protective framework that allows staff to travel with confidence and clarity. This policy can also be used to address ethical and environmental impacts, promote sustainable practices and ensure regular updates and traveller feedback. This not only enhances the safety and effectiveness of humanitarian operations, but also demonstrates the organisation's commitment to the safety of its personnel, building trust and morale among staff.

Travel approval systems

A well-structured travel approval system is a critical component of travel risk management. Organisations should determine what kind of travel requires what level of authorisation, which may involve several considerations including risk levels and travel distance. The ideal system is sustainable and relevant, while also adding value and improving risk management. A system that is too complex or resource-intensive may become burdensome, while one that is too simplistic may not provide adequate protection.

A travel clearance system encompasses several key elements, which can include the following:

- **Formalised request process.** The travel approval process begins with a formalised request where travellers submit detailed itineraries outlining their destinations, purpose and duration of travel and planned activities. This ensures that all relevant information is captured and reviewed before approval is granted.
- **Risk assessment.** Each travel request should undergo a risk assessment to evaluate the potential risks associated with the journey and destination, including political instability, health threats, environmental hazards and local security concerns. This also provides an opportunity for travellers to highlight any personal considerations that may need to be factored in.
- **Traveller preparation.** Ensure that travellers are adequately prepared with necessary tools and resources, such as travel insurance, medical supplies and emergency funds.
- **Post-travel debriefing.** An effective travel approval system usually incorporates a post-travel debriefing. It may be helpful for travellers to provide feedback on their experiences on their return, noting any incidents or observations that could inform future risk assessments or policy adjustments.

Other considerations

- **Internal capacity for travel risk management.** Some organisations have invested in internal capacity to manage travel and mitigate travel risks, for example having dedicated staff responsible for booking flights. This requires a sustained budget and specialist resources but can be highly effective in ensuring that travel risks are managed proactively and comprehensively.
- **Shared responsibility.** Both the organisation and the individual traveller have joint responsibility for travel safety and security. The organisation is responsible for creating and maintaining a system and environment of managed and safe travel, as well as establishing the capacity to respond and support travellers when things go wrong. The traveller is expected to listen to briefings and adhere to guidance and requirements.
- **Personal risk profiles.** A staff member's personal risk profile can play an important role in managing travel-related risks and should be factored into planning and preparedness. For example, staff with health conditions may need access to necessary medicines.

7.1.2 Modes of travel

Decisions on the mode of travel should be guided by a comprehensive risk analysis. For instance, while a short one-hour flight on an airline with a questionable maintenance record may present certain risks, it may still be a safer option than a 10-hour cross-country journey by road. The following sections should be considered in this context.

Air travel

Air travel presents several risks that organisations should be prepared to manage. These include health-related issues such as deep vein thrombosis (DVT), as well as security risks including hijacking or air accidents. Travellers may face stress due to delays, lost luggage and complex security screening procedures.

- **Airline safety and selection.** Not all airlines are equal in terms of airworthiness and maintenance quality. Several commercial organisations rate airlines globally, and this information can be used to make informed decisions. As a minimum, organisations should review airlines' safety procedures and records before using them.
- **Use of humanitarian airlines.** The UN Humanitarian Air Service (UNHAS) and other humanitarian airlines provide essential services in many challenging environments. Organisations wishing to use UN or NGO air services should be familiar with how they operate, including local rules and regulations, which can vary significantly from those of national carriers.
- **Traveller briefings and support.** Travellers usually need to manage many of the risks associated with air travel themselves, but organisations can still provide comprehensive briefings and guidelines. Contingency plans address common issues like flight delays, lost luggage or changes in security conditions. Commercial agencies may offer services including individual alerts and tracking.

Aircraft and maritime safety guidance checklist

Ensuring the safety and maintenance of aircraft and maritime vessels can be crucial for a successful journey. Here are some considerations, particularly for vessels that the organisation is chartering:

- **Maintenance history** – check that the aircraft or vessel has undergone regular and proper maintenance.

- **Spare parts for maritime vessels** – verify the availability of essential spare parts, including a secondary engine and a spare battery, in case of mechanical failure at sea.
- **Navigational and communication systems** – assess the functionality of navigational and communication systems to guarantee reliable operation during the journey.
- **Safety equipment** – check safety equipment, such as life jackets, distress signalling devices, torches, operational fire extinguishers, emergency oxygen masks, life vests and spare oars for lifeboats.
- **Fuel** – verify fuel sufficiency, including a reserve margin beyond the planned journey requirements, to account for unforeseen delays or detours.
- **Cargo weight** – confirm that cargo weight is within the vessel's safety limits and properly distributed for balance.

Road travel

Road travel remains the most common form of travel for humanitarian organisations – and it is also one of the most hazardous. The risks associated with road travel are numerous and varied, ranging from vehicle accidents and blockades to armed ambushes and poor road infrastructure. Travel by road can involve long journeys through difficult terrain, unpredictable weather conditions and regions with high levels of insecurity. Managing these risks requires careful planning, robust systems and a strong focus on the safety and security of both personnel and resources. The following considerations can be critical:

- **Vehicle fleets and maintenance.** Aid organisations' vehicle fleets are typically diverse, comprising SUVs, saloon cars, trucks and motorbikes of varying age and mileage. The condition and roadworthiness of these vehicles are paramount. Regular maintenance checks, including inspections of tyres, brakes and safety equipment, should be mandatory. Organisations will also want to ensure that vehicles are equipped with essential items such as spare tyres, jacks, first-aid kits and communication devices.
- **Visibility.** Consideration may need to be given to how visible an organisation wants to be while travelling, in line with the organisation's security strategy in the context. Organisations that wish to be visible as humanitarian actors will need to ensure that all vehicles are clearly identifiable through colours and logos (this may also apply to other types of transportation, such as boats).

- **Driver competency and training.** Drivers' competency, morale and connection to organisational values can be critical to ensuring safe journeys. Drivers should be aware of local driving norms and practices, which can vary significantly from one country to another. It is advisable to train drivers and regularly evaluate their performance. In areas of conflict or criminality, drivers may need to be trained in security and defensive driving, such as situational awareness, risk assessment and evasive manoeuvres.
- **Movement control systems.** Many organisations use log/time sheets for managing personnel and resources during road travel. Movement control (MovCon) systems track travellers and manage resources, with alert triggers and contingency plans for overdue or missing staff. These systems should be adapted to the context and continuously updated.
- **Digital tracking and journey-logging.** Digital tracking and journey-logging devices in vehicles provide enhanced safety features and detailed journey metrics, including live vehicle tracking. However, it is essential that such systems have proper oversight and protocols. They should be integrated into the overall travel risk management strategy and supported by a robust response capability in case of emergencies.
- **Road travel protocols and briefings.** Organisations should establish clear protocols for road travel, including guidelines on speed limits, safe driving practices and emergency procedures. Pre-departure briefings for travellers cover the specific risks associated with the journey, road conditions, the security situation in the area and local cultural norms and expectations.
- **Contingency planning for road travel.** Given the unpredictable nature of road travel, contingency planning is essential. Organisations should have clear protocols for responding to incidents such as vehicle breakdowns, road blockades and ambushes, alternative routes, emergency contacts and procedures for relocating/evacuating personnel. In high-risk areas, organisations may also consider using convoys or security escorts.

▶ *See Chapter 4.2 for more on armed escorts.*

- **Coordination with local authorities and communities.** Local police, military and community leaders may be a source of timely and accurate information about road conditions, security threats and other relevant factors. Other aid organisations, including UN agencies, may also be able to provide this type of information. Local communities may provide valuable support during travel, such as monitoring road conditions and providing assistance in case of accidents.

- **Environmental considerations.** Organisations may need to be mindful of the environmental impact of their operations. This includes minimising the use of vehicles, reducing emissions and ensuring that waste is disposed of properly. Environmental impact assessments may be advisable before undertaking large-scale road travel operations, or when considering purchasing or disposing of vehicles.

Public transport

For staff who are not residents in the area, the decision to use public transport, such as buses or taxis, should be based on a thorough risk assessment. In some circumstances – and especially in very high-risk contexts or where personal profiles place particular staff at heightened risk – this consideration may also need to apply to resident staff. For lower-risk destinations, travellers can be informed about safe transport options, including how to identify licensed and reputable service providers. In higher-risk areas, it may be advisable to avoid public transport altogether. Organisations should have clear policies regarding staff journeys to and from work, including whether the organisation will arrange or pay for transportation, rather than simply advising against the use of public transport without arranging alternatives.

Checkpoints

Interactions at checkpoints can range from supportive to hostile. Travellers may be harassed, intimidated or threatened by individuals controlling checkpoints, especially if they are easily provoked or under the influence of alcohol or drugs; or checkpoints may be friendly and can provide valuable information about road conditions ahead. The way staff interact with individuals at checkpoints can influence not only their own journey, but also how other aid workers are treated later.

It is essential for staff to quickly assess each checkpoint's type and location, and the mood of those managing and working in them. Common checkpoint locations include crossroads, bridges, mountain passes and town entrances or exits. The objectives of checkpoints vary and may include traffic control and security.

In a single vehicle, the journey leader can act as the spokesperson if they speak the local language. In a convoy, a leader can be identified for each vehicle – ideally the most experienced person with local language skills. Drivers often play a key role in initial interactions since they are typically the first to engage with checkpoint guards. All team members should be aware of the cargo and be consistent in explaining their organisation's mission and the purpose of their journey. It may be advisable for passengers to carry identification in the local language; avoid handing over passports if possible. If asked to enter a guardroom, staff should usually try to stay together and not leave the vehicle unattended.

▶ *See Chapter 7.4 for more on how to deal with harassment against staff.*

Road safety

Organisations can consider the following as part of their policies on road travel.

- Prohibition of weapons (in line with organisational policy and humanitarian principles)
  - Most humanitarian organisations do not allow weapons on board vehicles or other forms of transport, with exceptions for situations involving coercion. Responsible staff should ensure that this policy is clear and visible (e.g. stickers with crossed-out gun symbols).

- Engagement with armed actors
  - Assess and define the organisation's stance on using or engaging with armed escorts and other armed actors. This may have implications for policies prohibiting weapons on organisational vehicles (especially for aircraft and watercraft where any armed protection may not be in a separate vessel).
- ●Transporting non-affiliated passengers or cargo
  - Develop a policy for transporting non-affiliated passengers or cargo.
  - Provide laminated materials in local languages to communicate this policy.
  - Allow exceptions for practical considerations (e.g. guides, hospitality, medical emergencies).
  - Anticipate cultural requirements (e.g. women travelling with male relatives in certain contexts).
- Waiver of liability
  - Place a waiver of liability document in vehicles exempting the organisation from responsibility in case of unforeseen incidents.
  - Acknowledge the varying efficacy of such documents based on local laws and circumstances.
  - Consider the practicality and potential acceptance issues of implementing this policy.

Water travel

While often necessary in humanitarian contexts, such as during flooding or in the rainy season, travelling by water can be fraught with risks. Managing these risks requires careful planning.

- **Selection of watercraft.** Organisations should use vessels that are suitable for the specific conditions they will encounter, whether rivers, lakes or coastal waters. The vessel's condition, including its maintenance history and safety equipment, should be thoroughly inspected before use. Before each trip, check to ensure that there is sufficient fuel and a reserve.

- **Crew competence and training.** The competence of the crew is as important as the condition of the vessel. Check that crew members have the necessary licences, certifications and experience to operate the vessel safely. This includes training in emergency procedures, navigation and communication (see the box below).
- **Safety equipment.** Vessels should have essential safety equipment, including life jackets, distress signalling devices, fire extinguishers and spare oars.
- **Risk of piracy.** Additional precautions may need to be taken in regions known for piracy. This includes selecting vessels with advanced security features, such as surveillance systems and secure communications equipment. In some cases, armed protection might be necessary in order to safeguard the vessel and its occupants.

▶ *See Chapter 4.2 for more on using armed protection.*

- **Contingency planning.** Clear protocols can be put in place for responding to emergencies, such as mechanical failure, severe weather and piracy attacks. These protocols can include alternative routes, emergency contacts and procedures for evacuating personnel.
- **Environmental considerations.** Water travel can take place in sensitive ecosystems and organisations may need to be mindful of their environmental impact. This can include minimising pollution, avoiding disruption to local wildlife and ensuring that waste is disposed of properly.
- **Coordination with local authorities.** Coastguards, port authorities and community leaders can provide information about water conditions, security threats and other relevant factors.

Crew qualifications and competence checklist

Where organisations are chartering aircraft or water vessels, it is important to consider the qualifications of the crew.

- **Licences and certification**
  - Ensure that the pilot/captain and crew possess valid licences and certification for their roles and the type of vessel being operated.
- **Mechanical proficiency and emergency preparedness**
  - Evaluate the crew's mechanical proficiency and preparedness to handle unexpected situations.
- **Language proficiency**
  - Ascertain that the crew is proficient in languages essential for communication during the journey and in emergencies.

Unconventional travel

In challenging terrain and remote regions, conventional transportation may be impractical or impossible and staff may need to travel on foot or rely on animals. The following considerations are important for managing associated risks effectively.

- **Route mapping and risk assessment.** Routes should be meticulously mapped out to avoid hazardous areas. This can involve assessing the terrain, identifying potential threats and planning for rest points and water sources. Staff may need special training in handling potential threats, such as encounters with wildlife or hostile groups.
- **Traveller preparation.** Travellers should be prepared for both the physical and mental challenges that may come with this mode of travel. This can include ensuring they have the appropriate gear and supplies for the terrain and climate as well as being trained in survival skills, first aid and emergency communication.
- **Communication protocols.** Travellers should be provided with reliable communication devices, such as satellite phones or two-way radios. Regular check-ins should be established with the relevant organisational office. In

areas with limited or no communication infrastructure, organisations may need to develop alternative methods for tracking and supporting travellers, such as using local guides.

▶ *See Chapter 6.1 for more on communications.*

- **Coordination with local communities.** Local communities can share information and resources to navigate difficult terrain and avoid security threats, as well as providing support in case of emergency.
- **Contingency planning.** Clear protocols should be in place for responding to emergencies, such as injuries, equipment failure and encounters with hostile groups. Protocols can cover alternative routes, emergency contacts and procedures for evacuating personnel.

▶ *See Chapter 5.5 for more on medical emergencies.*

Convoys

A convoy is a group of vehicles travelling together, primarily for protection, support or efficiency. In humanitarian contexts, convoys are used to transport goods, personnel or equipment through areas with security risks or logistical challenges. They can consist of vehicles from a single organisation, or be arranged with other actors.

In low-risk areas, the size of a convoy may be less significant as long as there is reliable communication between all vehicles (e.g. using radios or walkie-talkies). However, in high-risk or complex environments the size and structure of a convoy may need to be carefully considered. While travelling in a convoy can reduce risks through strength in numbers, it can also present dangers, such as being mistaken for a military column, and may attract unwanted attention. Typically, a convoy has a lead vehicle, a main body where valuable assets are placed, and a tail vehicle. In some situations a scouting or point vehicle may be used, maintaining a safe distance and radio contact with the rest of the convoy behind it. The convoy leader is usually in the lead vehicle, with another experienced person in the tail vehicle.

Before departure, the convoy leader should ensure that all vehicles are checked for suitability, fuel, necessary equipment and documentation. It is advisable for drivers and vehicle leaders to be fully briefed on convoy rules, including speed, distance-keeping, communication protocols and procedures for handling various scenarios, such as checkpoints or vehicle breakdowns. Proper distance between

vehicles is crucial; they will usually need to be close enough to maintain visual contact but far enough apart to avoid getting caught in the same incident. The appropriate distance can vary depending on the terrain, weather and security conditions, and may need to be adjusted over the course of the journey.

7.1.3 Personal security considerations in transit

Airports, ports and bus and train stations can present significant security risks. These locations are frequently targeted for criminal activities, and travellers may be vulnerable due to unfamiliarity with the local environment and security conditions. Organisations can take proactive measures to mitigate these risks.

Pre-travel briefings should cover the security situation at the destination, relevant legal and administrative requirements (such as vaccination mandates), potential risks associated with airports, ports and bus and train stations, and include contact information for local security personnel. Additionally, briefings may cover the following:

- **Safe transport options.** Guidance can be given on transport options from airports, ports and bus and train stations to the final destination. This may include providing lists of legitimate taxi services or locations, reputable transport apps and arranging for pickup by a designated individual. Using organisational vehicles is recommended, as drivers are often familiar with local conditions and can provide a secure and reliable means of transport.
- **Personal security measures.** Travellers can be advised on personal security measures while in transit, such as keeping valuables out of sight, staying alert to their surroundings and avoiding interactions with strangers. Organisations may also provide travellers with personal security devices, such as alarm whistles or tracking devices. Travellers may need to be instructed on how to handle their luggage securely, including keeping it in sight at all times, using locks on bags and avoiding carrying large amounts of cash or valuables. Consideration may need to be given to labelling luggage without revealing personal details that could be used by criminals.
- **Navigating security checks.** Travellers may need guidance on how to navigate security checks at airports and stations. This can include understanding restrictions on carry-on items, knowing what documentation is required and when, and being aware of any specific security measures. Travellers should also be made aware of any potential cybersecurity risks during airport security processes and what precautions they can take to protect sensitive information.

- **Dealing with authorities.** In some cases, travellers may be questioned or experience other potentially difficult interactions with authorities. Organisations may want to provide guidance on how to handle these situations, including being cooperative and patient, being truthful and knowing when to request legal or consular assistance. Travellers should be aware of their rights and the local laws governing their stay.

General operational safety and security travel checklist

When planning staff travel, particularly in complex environments, the following general considerations should be taken into account:

- Weather conditions
- Security conditions at different locations
- Clearance from authorities
- Contingency plans
- Identification (travellers and vehicles)
- Reasonable assurance that the transportation mode, such as a vessel, is not also being used to carry out illicit activities, such as smuggling

7.1.4 Hotels and temporary accommodation

Travellers may find themselves in need of overnight accommodation in hotels or temporary lodging. Where no advance planning has been possible, staff should know how to assess the security of the accommodation and request changes as needed.

- **Hotel security infrastructure.** Hotels that provide the following measures are generally better equipped to respond to emergencies and protect the security of their guests: security personnel, 24-hour reception, comprehensive access control systems and visible, operational fire safety systems.
- **Room selection.** Travellers should choose rooms in well-trafficked corridors with good visibility. Rooms that are easily accessible to intruders or located in isolated areas should be avoided. Access points, including doors and windows,

may need to be checked to ensure they are in good working condition and can be securely locked.

Considerations during a stay include the following:

- **Emergency preparedness.** Travellers should familiarise themselves with the accommodation's emergency procedures, locate the nearest exits and ensure they have access to a basic emergency kit (including a torch, first-aid supplies and emergency contact numbers). Travellers should also know the location of fire extinguishers and other safety equipment.
- **Visitor interactions**. Travellers may need to exercise caution when interacting with visitors at the accommodation. This can include not allowing entry to individuals whose identity or intent is unclear, such as new acquaintances, unsolicited service staff and personnel delivering items. If a visitor appears suspicious, security personnel (such as hotel security) should be notified immediately.
- **Reporting concerns.** Any concerns regarding hotel room security or the behaviour of hotel staff or other guests should be reported promptly to hotel management. Organisations can provide travellers with guidance on how to escalate these concerns if necessary, including contacting local authorities and organisational security personnel.
- **Cultural considerations.** Travellers should be mindful of local cultural norms and expectations when staying in hotels and temporary accommodation. This can include respecting local customs related to dress, behaviour and interactions with hotel staff.

▶ *See Chapter 7.2 for more on site security.*

7.1.5 Contingency planning and incident management

Robust contingency planning and incident management are essential. An important part of this is developing – and regularly reviewing and updating – comprehensive plans that can be quickly implemented in response to emergencies. This usually involves identifying potential risks related to travel (paying close attention to personal risk profiles), developing strategies to mitigate these risks and establishing protocols for incident response. Regular training and drills can help with preparedness.

▶ *See Chapter 4.3 for more on contingency planning.*

▶ *See Chapter 4.4 for more on incident response.*

▶ *See Chapter 5.4 for more on staff care.*

▶ *See Chapter 5.5 for more on medical considerations.*

Further information

Guidance and resources

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

Davis, J. et al. (2020) 'Module 10, Travel safety: airports, vehicles and other means of transport' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/).

GISF (2024) *4. Travel and movement*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/4-travel-and-movement/).

IASC (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys).

International Organization for Standardization (2021) *ISO 31030:2021: Travel risk management – Guidance for organizations* (www.iso.org/standard/54204.html).

7.2 Site security

Site security can deter or stop intrusion, delay attack and mitigate the effects of an incident in the immediate vicinity of a site.[97] This chapter focuses primarily on offices and residences for staff living away from home. It is also necessary, however, to consider site security for locations where staff spend a significant amount of time, such as project sites, refugee camps, school buildings, medical facilities and distribution points. Site security measures may sometimes also be needed around the private homes of staff.

7.2.1 Site selection

Site protection starts with identifying and selecting a suitable location, bearing in mind that the perfect choice seldom exists. In addition to space, price and other criteria, the physical strengths and weaknesses of a site can be assessed from a security point of view – what is acceptable, what must be improved and how much this would cost. This allows an organisation to assess suitability and to detail and negotiate any permissions to make alterations before signing a lease.

Security approaches

In any physical security review, whether selecting a site or adding new physical security measures, it is important to consider the local community's perceptions and attitudes towards these measures. For instance, constructing a 2.5-metre wall may be advisable from a protection perspective but may raises suspicions or be disruptive to the local space. This 'acceptance lens' can be applied to all examples of good practice shared in this chapter.

Individual profile considerations

When selecting offices and accommodation, it is important to consider the personal profiles and needs of staff and likely visitors. This can help create a secure, inclusive and supportive work environment.

In certain contexts, it may be culturally inappropriate or potentially unsafe for female staff to live alone. In such cases, shared living arrangements that align with social norms and meet the needs of female colleagues may be appropriate. Providing separate quarters for male and female staff might be advisable, depending on the cultural and social context. Accessibility requirements for

97 The risks change dramatically in situations of insurgency and war, where additional measures are required. These are considered in more detail in Chapter 7.10.

disabled staff are also an important consideration. Providing options for private or shared accommodation that respects gender identity and sexual orientation can help mitigate risks and ensure a welcoming environment.

Consulting with diverse groups of staff when choosing sites can help ensure their needs are adequately met.

▶ *See Chapter 1.2 for more on inclusive security considerations.*

Physical criteria

Organisations can consider various physical criteria when selecting a site. This may include the following:

- **Structural resilience.** It is advisable for organisations to ensure that buildings are sufficiently robust and resilient to withstand the impacts of extreme weather and other environmental risks, including floods and landslides. This can involve checking the structural integrity of the building, the quality of materials and the effectiveness of drainage systems in the area.
- **Location.** Organisations may want to avoid areas that offer opportunities for concealed approaches and escapes – for instance those with dense vegetation or narrow and poorly lit alleyways. Areas with many unoccupied, damaged or derelict buildings may also present risks. In situations of active armed conflict, site selection criteria will often include considerations of distance from potential military targets and access to shelter facilities. While security concerns may drive the selection of affluent neighbourhoods, diplomatic enclaves or gated communities, these choices could convey an elitist image, potentially affecting how the organisation is perceived.
- **Security perimeter.** A double perimeter, where a building or apartment is situated within a compound or a larger gated area, is generally preferable. An effectively managed perimeter can act as a deterrent to unauthorised access and provide early warning in case of intrusion.
- **Emergency evacuation.** How easily can staff and visitors evacuate the building or immediate area in the event of an emergency, such as a fire? Consider exit routes, whether the building's design facilitates the safe and swift evacuation of all occupants, and whether the local fire brigade can access the site efficiently.
- **Floor level.** It is often advisable to rent office space or an apartment above the ground floor to reduce vulnerability to intruders. However, higher floors may be unreachable by emergency equipment and difficult to escape from.

If the roof is accessible, perhaps from a neighbouring building, occupying the apartment directly beneath could increase risks.

- **Accessibility.** Ensure that entrances, exits and common areas are accessible to those with mobility challenges, and that emergency procedures account for their needs. Considering whether the building is equipped with features such as ramps, elevators and accessible restrooms is advisable.
- **Secure parking.** It may be prudent to confirm that the site provides secure parking facilities: the parking area is well lit, monitored by security cameras and protected by controlled access points, such as gates or barriers. Secure parking is an important aspect of the overall security of the premises, particularly during non-peak hours. Parking spaces can also present risks in active conflict settings, and these are discussed in more detail below.

▶ *See Chapter 7.10 for additional site considerations in active combat areas.*

Building ownership, occupancy and tenancy

- **Ownership of the building.** Organisations should ascertain the ownership of the building, for example whether it is held by an individual, a bank, a shop or a religious organisation. Understanding the owner's identity and their potential role within the community may provide insights into how their affiliations could impact the organisation's image and operations.
- **Occupancy and tenancy.** When evaluating a building, it is advisable to consider who else occupies or rents space within the premises. The presence of other tenants might offer added awareness and a degree of collective protection. However, other tenants could introduce risks, particularly if they are or might become targets themselves. A single-tenant site may be more fully under the organisation's control.
- **Other organisations.** Security advantages and efficiencies can sometimes be gained if several aid organisations occupy sites in the same place or close together. UN agencies, for example, often group their offices in a single area to enhance security and reduce costs. Some NGOs have also adopted this approach. However, grouped sites may evolve into gated communities, potentially isolating organisations from the broader community, or create the impression of close association between organisations, which may impact local perceptions and acceptance. The concentration of possible targets within a single area means that an attack may have a much larger impact if successful.

The neighbourhood

It is advisable to examine the surrounding area, ideally within a radius of at least 1.5km, to gain a comprehensive understanding of the neighbourhood. Key considerations include the following:

- **The stability and social cohesion of the resident population.** High social cohesion might suggest a reliable, informal neighbourhood watch scheme, with residents who are vigilant and concerned about security. Low social cohesion could indicate a lack of interest in neighbours' security, potentially allowing strangers easy access to the site.
- **The nature of the neighbourhood.** Are most people local residents, or do large numbers of workers or travellers frequently pass through? The less local the population, the easier it may be for outsiders to enter the area without attracting attention.
- **Availability of local authority and rescue services.** Determine the locations of the nearest fire station and police posts and the residences of influential local leaders. Identify the areas police patrols cover most frequently.
- **Access control measures.** Consider the type of access control used by local residents, including how they enter and exit premises and whether there are physical or virtual/computer systems in place. Are guards stationed outside homes? Are homes in the area heavily fortified?
- **Crime levels.** Criminality may be an important factor, keeping in mind that crime levels can be high in both affluent and less affluent areas. Regardless of the area's wealth, organisations and their staff should avoid the appearance of wealth. Whether or not to select a location near a police station depends on the context and the relationship between the police and the local community.

In general, cultivating good relations with neighbours, without being intrusive, can be an important site security measure. Establishing even a basic relationship may increase the likelihood of neighbours acting if they observe something suspicious.

7.2.2 Site reinforcement

With regard to the physical security of work and residential sites, a useful rubric is 'Deter, detect, delay and respond'.[98] This can include: adding elements to make a building harder to enter, such as walls, bars and access controls; removing

98 GISF (2024) *3. Site security.* NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/3-site-security/).

elements that make it hard to see potential intruders and adding cameras, alarms and watchmen; having a saferoom that can delay intruders' access to staff; and putting procedures in place to quickly respond when intrusions are detected. The following sections cover these measures in detail.

The outer perimeter

The following are factors when considering the security of the outer perimeter of a site.

- **Surroundings.** If the vegetation surrounding the building provides potential access or hiding places, organisations can consider trimming, cutting or replacing it with thorn bushes. Rubbish or rubble near the perimeter could potentially assist an assailant in monitoring or gaining access to the building, or hinder the response of security personnel. Prompt removal of any debris that could conceal explosive devices is also advisable.
- **Walls and gates.** Constructing walls around the site may enhance security. Good practice generally suggests that these should be at least 2.5 metres high and fortified with additional measures such as barbed wire or broken glass along the top. Nearby trees or other objects that could make scaling the walls possible may also need to be addressed. Gates, as potential vulnerable points, should be properly secured, with peepholes for visual verification of visitors. In some contexts having a secondary, but secure, exit point might be prudent.
- **Lighting and visibility.** Improved lighting can serve as a deterrent to potential threats, but care should be taken to strike a balance between enhancing visibility and drawing attention. Lighting should also not negatively affect neighbours. Sensor lights that activate upon detecting movement may be a good option, provided they have a consistent power supply. In areas prone to power outages, alternative energy sources like generators or solar lighting might be considered. The decision to display the organisation's logo on the outer perimeter will depend on whether the organisation has determined that visibility in the given context enhances or detracts from its security. In environments where the organisation is well regarded, displaying the logo can be appropriate, accompanied by translations in the local language.
- **Unoccupied sites.** For sites that are unoccupied for periods of time, organisations may implement measures to create the illusion of activity, such as periodically turning lights on and off and adjusting shutters to deter potential intruders.
- **Consistency with local security practices.** Adopting similar levels of site protection as other buildings in the vicinity, even if perceived risk levels do not seem to warrant it, could be advisable.

- **Parking and vehicle access control.** Parking arrangements should be designed to prevent unauthorised vehicle access to the site, and reduce the risks of attacks on vehicles. Where risks such as vandalism, car theft, mob violence or bombing are present, vehicles are best parked in secure locations, such as within a compound. It is also advisable to ensure sufficient parking space when selecting a site, and that vehicles are locked when not in use. Operating procedures for vehicle key control, parking arrangements and emergency use should be established. Parking and fuel arrangements should facilitate easy departure from the site. This can mean ensuring that vehicles are fully fuelled at the end of each day and parked to allow quick loading and exit.

Crime prevention through environmental design

Crime prevention through environmental design (CPTED) focuses on improving site security by manipulating the physical environment to guide behaviours and reduce the opportunity for crime. This is often overlooked during the design or renovation of facilities, or when security solutions are developed over time. CPTED strategies include the following:

- **Natural surveillance.** Increasing exterior and interior visibility to expose would-be perpetrators and enhance the sense of safety for legitimate users. It involves carefully managing landscaping, lighting and placement of windows and entrances for clear sightlines and to reduce opportunities for concealment.
- **Natural access control.** Utilising physical elements like structures, barriers, landscaping, lighting and signage to direct access to specific, controllable points.
- **Territorial reinforcement.** Defining public, semi-public and private spaces through physical elements like buildings, fences and landscaping. This encourages occupants to challenge intruders and makes them more easily identifiable.
- **Maintenance.** Avoiding visible signs of disorder like broken windows, graffiti and discarded equipment, which can create an impression of abandonment and neglect that invites criminal activity.

- **Bollards and anti-ram barriers.** Strategically placed, bollards may restrict vehicle access but still allow pedestrian flow. Bollards can be fixed, removable or retractable. Anti-ram barriers can provide enhanced protection against vehicle-borne threats and are usually designed to withstand high-speed impacts. Options include reinforced concrete barriers, steel bollards and cable systems. Bollards can be integrated into the overall perimeter security system, complementing walls and gates.
- **Integration of perimeter security measures.** By using a combination of physical barriers alongside other security measures, organisations can establish a layered defence. Aligning these perimeter security measures with the organisation's broader security objectives, including fostering acceptance and goodwill among the local population, is crucial to ensuring a cohesive and comprehensive approach to safeguarding personnel and assets.

The inner perimeter

It is advisable for organisations to assess each site from the perspective of an intruder, identifying any potential weak spots, particularly around doors and windows, but also garage doors and cellars.

- **Entrance doors.** Organisations may want to ensure that entrance doors are strong, including the frames and hinges. If any glass is present in the door, consider replacing it. Installing an optical viewer (peephole) along with a primary and auxiliary lock on outer doors can enhance security. For additional internal security, organisations can consider installing a safety chain and a sliding deadbolt or strong bar across the door. Heavy-duty padlocks, placed at the top and bottom of the door with welded padlock rings, can provide further protection. Finally, it is advisable to position panic buttons or telephones away from entrance doors to prevent an intruder from blocking access to them.
- **Windows.** Organisations may want to secure windows, particularly on the ground floor, with bars, grills or shutters provided they are easy to open from the inside in case of an emergency. If upper-floor windows are accessible from the outside, it may be useful to secure them with bars or grills. It is important to ensure that these cannot be easily unscrewed or removed from the outside.
- **Night-time routine.** It may be advisable to close curtains at night to prevent intruders from observing who and how many people are inside the building. Staff may wish to leave a light on when departing the premises to create the impression that someone is still inside. All locks and bolts should be checked to ensure they are in good working order and should be routinely locked as night falls or before going to bed.

- **Alternative exit in emergencies.** In case of fire, intrusion or rioting, it is advisable to have an alternative exit from the building. This escape route, including any window protections, should be easily accessible from the inside, taking into account the personal profiles of all staff (such as mobility needs). If bars are already fitted to windows, organisations may want to modify them to allow easy exit from the inside. This could involve hinging the bars on one side and securing them with a padlock, ensuring that occupants can quickly access the key in case of emergency.
- **Burglar alarms and closed-circuit television (CCTV).** While burglar alarms and CCTV cameras may be uncommon in many aid contexts, organisations could still consider using these for additional security. Both typically depend on an electricity supply, though some burglar alarms operate on batteries. CCTV cameras may offer limited deterrence unless intruders are aware of their presence and function, and there is a reasonable chance of being caught. High-decibel security devices, which operate remotely and directionally, create an unbearable sound that can stop intruders or even rioting crowds from advancing further into the premises. They are usually equipped with sabotage protection and operate on batteries.

Basic fire safety considerations

To address the risk of fire, consider the following:

- Fit smoke and carbon monoxide alarms and place fire extinguishers in the kitchen and on every floor – electrical and oil fires require a CO_2 or powder-filled extinguisher; for other types of fire a foam or water-filled extinguisher should be used.
- Check extinguishers and have them serviced at least once a year.
- Identify fire escape routes and ensure that, when locked from the inside, they can be opened instantly.
- Organise regular fire drills, especially if staff turnover is high.
- Make sure that gas room heaters are properly vented and check that they have thermocouples (devices that prevent the gas supply from turning on without a pilot light or other source of ignition) – heaters without thermocouples should not be left unattended and should not be used at night.

- Formally designate trained individuals to ensure that disabled staff are assisted in case of an emergency (sometimes described as a 'buddy system'); these individuals should be staff who spend most of their time on site.
- Place evacuation maps so that they are prominent but not visible to passers-by and perhaps code the identification of rooms so that it helps staff and visitors without also serving as a potential guide to intruders.

Safe rooms

A safe room can serve as a critical refuge for occupants during emergencies, providing protection from intruders until help arrives. Most safe rooms are not designed to withstand bomb or shell impacts.

- **Location and accessibility.** A safe room should be easily accessible and ideally situated in the core of the building for quick entry. Alternatively, upper floors can be converted into safe areas by securing staircases with locking grills during vulnerable times, such as at night.
- **Security features.** The safe room should ideally be equipped with reinforced doors and secure windows to deter intruders. A telephone or emergency radio should be available to summon assistance. Organisations may want to consider installing uninterruptible communication systems to maintain connectivity during power outages. A list of key contact numbers, including emergency services and internal response teams, can be prominently displayed within the safe room.
- **Emergency supplies.** The safe room should be stocked with essential supplies to sustain occupants during an emergency. This can include first-aid kits, a small quantity of water, non-perishable food items and sanitary provisions. Chairs, mattresses and bedding can be added in case staff have to take refuge for longer periods or overnight. Perishable items and medicines should be regularly checked and replaced.
- **Training and drills.** Regular training sessions and drills (including simulated scenarios) familiarise building occupants with the safe room's location, layout and procedures, including how to access it quickly and what to do while sheltering in the safe room during an emergency.

- **Communication protocols.** It is advisable to establish clear communication protocols within the safe room, outlining procedures for contacting emergency services and coordinating with external responders. Designating individuals responsible for initiating communication with authorities and providing updates on the situation is beneficial. A communication hierarchy can help to streamline information dissemination and decision-making.

▶ *To learn more about communications security, see Chapter 6.1.*

7.2.3 Site security risk management

Individual awareness

Site security is everybody's responsibility. Everyone – including receptionists, telephone operators, cleaners and gardeners – should be attentive and report anything unusual or suspicious, as well as breaches in security procedures (for example, doors or windows left open or keys left lying around). For residential properties, this includes all residents (including family members). These individuals should receive guidance on not letting unknown people into the property, giving information to unknown callers, giving details about the office layout or allowing their keys to be duplicated. Receptionists can play a key role in monitoring visitors and telephone calls, as well as letters and parcels being delivered, and can be trained to report anything and anybody that appears suspicious.

Guards

Aid organisations sometimes use guards for their residences, warehouses and offices. Guards may either be hired directly or contracted from a local provider. They can be ineffective if they are untrained, poorly instructed, poorly paid, poorly equipped or poorly managed. This is unfortunately not uncommon in many of the contexts in which aid work takes place. It is also not uncommon to find a bed in the guardhouse of aid organisation compounds, increasing the likelihood that the guard will fall asleep on duty. During the day, guards might be busy doing other things and may be distracted. When hiring guards, it is important to provide clear terms of reference and make this part of the contract.

In recruiting and managing guards, consider the following:

- Obtaining reliable references and, if possible, recruiting staff from the immediate neighbourhood. This can ensure that they are familiar with the area and its regular occupants and may increase their motivation to identify potential wrongdoers.

- Checking the language abilities of potential recruits. The primary occupants of a building need to be able to communicate with the guard.
- Hiring and deploying enough guards to detect intrusions and to support each other while working together.
- Ensuring that guards receive a full introduction to the organisation.
- If the guard is to carry a weapon (lethal or otherwise), the circumstances under which it may be used should be governed by the contract signed with the individual or the guard provider and reflect the organisation's security policy. It is recommended that such policies be reviewed by the organisation's legal adviser. Organisations can include contractual stipulations against the use of harmful substances (e.g. alcohol) while on duty and against additional jobs that may affect the guard's performance.
- Providing essential equipment, instruction and training. Equipment may include rain clothes, torches, a whistle or other alarm and a handheld radio or separate telephone in the guardhouse.
- Providing a logbook with instructions on keeping the log and reporting suspicious activity, as well as a list of key contact numbers.
- Providing clear instructions and training on how to deal with visitors and what to do if guards come across an intruder.
- Providing clear instructions about monitoring the surroundings, patrolling the compound and rules regarding gates, doors, windows and keys.
- Guards normally only have access to the outer (not the inner) perimeter, especially at residential premises. At the office building, they should usually have access to corridors, staircases and the roof, but not necessarily to the offices themselves.
- In areas where trespass or robbery is a high risk, consider routine inspection schedules alternated with rounds at less predictable times. Spreading guards out, with at least one in a position where they cannot be easily observed and overpowered – for example on a roof terrace – can be beneficial.
- Trained specifically for guarding purposes, dogs can be an excellent early warning of intruders and often a deterrent. However, a dog is potentially dangerous to people it does not know, and control measures may be necessary to protect legitimate visitors and staff.

Managing access

Access control starts with establishing key management control measures. Organisations may also use magnetic access cards, cipher locks (electronic push-button systems that allow entry only to people who know the code), magnetic readers, smart cards or biometric devices. Larger offices, typically in bigger cities, may control access by installing doors or turnstiles that operate with magnetic cards. Management controls should ideally be put in place for all of these. Systems can be expensive and may fail if the power supply is interrupted or if the mechanism malfunctions.

Site keys

Organisations can maintain a comprehensive log of keys and who holds them, and ensure that the number of keys in circulation is strictly controlled. If there is any doubt concerning key security, changing the locks is advisable. Keys can be labelled in code so they cannot be easily identified. Spare keys should be securely stored in a locked key box with a glass front that can be broken in case of emergency.

All personnel with access to keys, including household staff, should be informed of any key management protocols – for example, carrying keys on their person rather than leaving them on desks, in cars or in unattended coats and bags. Keys generally should not be duplicated unless explicitly instructed by the organisation's management, and any loss of keys should be reported immediately.

Being overly strict with key control can introduce its own hazards. For example, staff may be unable to escape from a burning building if they do not have access to the key for the emergency exit door. Similarly, a response to an emergency call from a colleague may be delayed if vehicle keys are locked away.

With regard to visitors, access control generally serves two functions: to establish the purpose and legitimacy of a visitor and to ensure that visitors do not constitute a threat. In some circumstances, access may have to be very

strictly controlled; visitors may be actively discouraged or directed to a separate building away from the organisation's main facility. In any case, it is helpful to have a designated visitor waiting space. This should be easily visible to security personnel and the receptionist. It should be connected to a toilet facility, but no uncontrolled access to the building should be possible for a visitor still waiting for clearance.

There are degrees of security control. For example, having visitors sign in and out is hardly a security measure in itself, as anyone can still get in. Stricter standard procedures might include ensuring that:

- all staff wear visible photo ID when on the premises;
- all visitors show identification;
- all visitors are given an ID or a pass, collected when they leave;
- no visitors are allowed in unless there is explicit authorisation from the person they want to see or who agrees to see them; and
- no visitors are allowed in unless accompanied by a staff member.

Stricter procedures include checks of visitors' bags and manual or electronic body searches (female guards and special training are usually needed for this).

In high-risk environments, anyone unknown, unauthorised or unable to provide convincing identification should not be let in. Initial cursory checks to establish whether a visitor could present a threat should take place at the outer perimeter, before they are admitted into the inner perimeter of a building. Only when a visitor does not seem to present a threat should they be let in. Establishing the purpose of the visit, contacting the host department, registering the visit and issuing a visitor's pass can then be done as a distinct second step within the premises, thereby minimising the number of people waiting at the main entrance. If in doubt, guards should be instructed to contact a supervisor.

In the event that a suspicious or unauthorised individual is encountered, security personnel or focal points should be alerted immediately. Protocols could be in place for notifying personnel promptly and discreetly, for instance through radios or panic buttons. Security personnel may consider introducing code words for summoning help discreetly. If the situation escalates or poses a significant threat, a lockdown may be necessary to secure the premises and protect staff. It is recommended that lockdown procedures are clearly outlined to staff, detailing actions to be taken, such as securing doors and barricading entry points.

Access policy: questions to consider

- **Should visitors' vehicles be allowed into the compound (if applicable)?** It may be worth considering where visitors should park. For instance, in the event of a bomb threat it is advisable to ensure that no non-organisational vehicles are present within the compound. Organisations may also want to consider prohibiting visitor parking around the building. Guards may be instructed to search vehicles, but this is a skilled task and requires proper training.
- **What is the organisation's policy on visitors bringing bodyguards or weapons onto the premises?** Organisations may choose to have a policy regarding the presence of weapons on organisational premises, taking into account the context and the type of visitor (e.g. police or government officials), and whether visitors arriving with their own bodyguards should be permitted to bring them into the premises. The potential liability of the organisation in the event of an attack on a visitor whose bodyguards were not permitted entry may need to be considered. Holding meetings in an annex of the building or on a veranda, where bodyguards could remain nearby, may provide a practical compromise. Guards should be trained on how to handle these kinds of circumstances.
- **How should access for service personnel and deliveries be managed?** Service access warrants careful consideration, including access for maintenance, repair, utilities personnel and deliveries. Decide whether service personnel should be allowed onto the premises in the absence of relevant staff, and whether arrivals can be planned and scheduled in advance. Requiring identification from service personnel could enhance security and, in the case of street vendors, staff may want to purchase goods outside the gate to limit access.

▶ *See Chapter 4.2 for more discussion on armed protection.*

Beyond traditional access control measures like visitor sign-in, there is a growing trend towards biometric authentication methods, such as fingerprint or iris scanning. Incorporating biometric authentication into access control procedures

can bolster their security posture while maintaining efficiency and convenience for legitimate visitors and staff members. Some organisations have opted for two-factor authentication (e.g. biometrics and a card), or created different authorisation levels for different facilities or departments. Organisations need to consider the risks of power failures, as well as the sensitivity of biometric data collection and potential risks of data breaches. Improper storage or encryption of biometric data could lead to identity theft or other privacy violations if the data is breached. These risks can be managed through proper data storage, encryption and system security measures.

Threatening phone calls and letters

Problematic phone calls can range from crank calls to sexual harassment and bomb threats. Where this is a risk, staff should be trained in how to respond. Using caller identification technology or call tracing can aid in identifying the origin of problematic calls and assist in investigations. Sexual harassment calls made to women can sometimes be stopped by having a male co-worker or co-resident answer the phone. If the caller persists, it may be best to change the telephone number. As a general rule, staff should not share their personal phone numbers and only give their work number on their email signatures and business cards.

In the case of threatening calls, recipients should try to remain calm and polite; refrain from sharing personal or sensitive information; give as little information as possible to the caller; listen attentively to gather as much information as possible to help with the caller's identification; write down all relevant details, including the name and phone number, if known; and report the threat immediately. If the call is a bomb threat, the key question will be when and where the bomb will explode. Unless confident that the threat is not real, the building should be immediately evacuated. If the office receives a threatening letter, it should be treated seriously and shared quickly with senior managers, the authorities and other organisations in the area, as appropriate.

Suspicious letters or parcels

While not a common threat to aid organisations, it is possible that a letter or parcel may be delivered that is deliberately contaminated with a poisonous chemical or biological substance, or that contains explosives. Possible indicators are traces of powder on the envelope, a strange odour and, in the case of a bomb, a ticking sound or visible wires. The parcel may be unusually heavy for its size, the address may be misspelt or the letter or parcel may be addressed to someone who no longer works for the organisation. It may lack postage or may have excessive postage, indicating that it was not assessed for postage at a post office.

Any such letters or parcels should be left where they are, the room vacated and security personnel alerted. Anyone who handled the object should be instructed to wash immediately with soap, especially their hands. The letter or parcel may have to be destroyed or opened by specially trained security personnel with proper equipment (contamination with a poisonous substance requires fully protective gloves as a minimum, and possibly fully protective face masks, as some substances may enter the body through inhalation).

7.2.4 Distribution sites

A number of measures can help increase security for staff and target populations at distribution sites.

- **Understanding the target population.** Gaining a good understanding of the target population is helpful, including how the population, as well as others in the vicinity, may perceive the distribution, whether there are potential tensions between groups and the likelihood of political interference. Staff could look out for any signs of desperation for the items being distributed, and identify elements that could have an interest in manipulating the distribution process.
- **Perimeter and site management.** Establishing a well-defined perimeter can be beneficial. Fencing or walls may be appropriate, or barricades with additional monitoring.
- **Location of the distribution site.** It may be advisable to choose a location where ambient traffic, both vehicular and pedestrian, is not obstructed, and ensuring the site does not attract unwanted bystanders or disturbances.
- **Managing entry and exit points.** Designate one entry point and one exit point. Effective management of crowds at the entry point can allow for swift separation of legitimate aid recipients from those who may not be eligible. Ensure sufficient staff are in place to manage unruly individuals. Exit points should be managed carefully, ensuring that recipients can leave the site in a safe and orderly manner.
- **Crowd control and movement.** Keeping people moving is important. Staff or authorities can monitor the area to prevent crowds, including family members assisting recipients, from gathering and impeding the departure of others. The safety and protection of those leaving the site, particularly women and young children, should be considered. Carrying large bundles, for example, may make aid recipients more vulnerable to potential targeting, and staff could consider ways to make distributed items less conspicuous.

▶ *For more details on distribution risks see Chapter 7.6 on civil unrest.*

Further information

Guidance

Davis, J. et al. (2020) 'Module 8, Security of facilities' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (https://gisf.ngo/resource/security-to-go/).

GISF (2024) *3. Site security*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/3-site-security/).

International CPTED Association (n.d.) The International Crime Prevention Through Environmental Design Association (www.cpted.net/).

Safer Edge (2014) *Office closure*. EISF (https://gisf.ngo/resource/office-closure/).

Source8 (2015) *Office opening: a guide for non-governmental organisations*. EISF (https://gisf.ngo/resource/office-opening/).

7.3 Cash security

Although the widespread adoption of digital money has generally reduced the amount of cash that organisations need to hold and handle, in many contexts and circumstances it is still necessary to hold, move and make transactions in cash. This chapter concerns multiple aspects of cash security, from theft and robbery to risks associated with cash programming.

7.3.1 Risks

While cash-related risks and their management are often the responsibility of finance and managerial staff, cash-related activities carry with them significant security risks. Withdrawing or transporting large amounts of cash makes aid workers vulnerable to robbery and theft. Travelling with cash, especially in remote or conflict-affected areas, increases the risk of being targeted by criminal elements or armed groups. The security risks of cash programming also need to be considered and addressed, including risks around transferring funds to aid recipients, fraud and reputational damage.

7.3.2 Risk mitigation measures

An essential first step is to carry out a risk assessment on the flow of cash around the organisation, followed by the design and implementation of mitigation measures at points of high risk.

The following section highlights measures to address risks associated with cash-related activities. These should ideally be decided and implemented collaboratively by security and finance staff.

Reducing the use of cash

Organisations can reduce their use of cash by making payments by cheque, bank transfer, pre-paid cards, credit cards or other electronic payments. No method of payment is risk-free, and it is important to establish guidelines on using credit cards and monitoring these regularly. Organisations dealing with sizeable transactions should consider taking out insurance specifically against loss or theft.

Risks of electronic transactions

There are several ways to transfer money without the use of cash. The risks associated with these mechanisms relate more to financial, operational or digital security, though there can be knock-on effects on staff security, for instance if a delayed transfer causes friction with parties expecting payment. Digital money transfer services and mobile apps can be vulnerable to hacking, phishing attacks and other forms of fraud and cybercrime. Informal systems known as hawala came under pressure post-9/11 over concerns that some transactions assist in the illegal transfer of funds to proscribed groups. Counter-terrorism legislation and bank de-risking practices have placed additional burdens on organisations trying to move large sums of money, in some cases forcing organisations to revert to using cash.

One specific risk around electronic financial payments is the targeting of transfers from donors to organisations or payments within organisations. Criminals are aware that very large sums of money are sent from donors to operational organisations, and also between head office and programme offices. Criminals could intercept email exchanges, clone staff accounts and issue false instructions to divert payments to external bank accounts. Last-minute changes or instructions in relation to significant bank transfers can also indicate fraudulent activity.

▶ *See Chapter 6.2 for more mitigation measures around digital security risks.*

Exercising discretion

When dealing with cash, discretion is important. The fewer people who know, the lower the risk. Communications that can be intercepted can be changed into some form of code. If withdrawing money from a bank, the transaction should be arranged discreetly in advance; avoiding making withdrawals at regular times or on regular days (e.g. in advance of monthly salary payments) can reduce risk. Paying suppliers is best done using one of the non-cash methods mentioned above, particularly for large sums. If staff regularly use the same hotel or supplier, organisations can consider setting up an account.

In some economies, and in cases of hyperinflation, the sheer bulk and volume of cash can present a problem. Even relatively modest amounts of international currency can translate into substantial bundles of local notes. When withdrawing cash from a bank, staff can try to have money paid out in higher denomination notes, and should consider the practicalities of transportation and storage.

Guidance for staff on good practice in cash security

- Do everything possible to limit the use of cash.
- Ensure reasonable credit limits and cash withdrawal limits.
- Check bank statements and investigate any unrecognised payments.
- Keep lists of phone numbers to call in case of loss or theft of credit cards.
- Block or cancel a credit card as soon as it is lost.
- Keep PINs safe.
- Keep credit cards in sight when handing over to pay for a purchase.
- Do not resist when confronted by a robber.

Limiting exposure

There are several ways to reduce exposure to loss or theft. Just-in-time payments to suppliers reduce the amount of time cash is held in the office. Another common practice is to set a ceiling on the amount of cash that can be withdrawn, transferred or kept in the organisation's safe. However, reducing the size of individual transactions will probably increase the number of transactions that need to be made, increasing costs. If cash is at most risk when it is being physically moved, organisations should consider moving larger amounts less frequently, particularly if more secure ways of transporting it are periodically available, such as helicopter flights or large convoys. Organisations can also consider the risks at different points in the transfer chain, from the bank to the organisation's safe to the eventual recipient, and represent this chain in a flowchart. It may be possible to reduce the number of links in the chain, for instance by asking suppliers to come to the office to receive payment rather than taking cash to them.

If burglary and robbery are risks, it is advisable not to keep all the money in one place, and have a certain amount to hand in an obvious place to satisfy and distract robbers. Some money should be easily accessible; the rest is better hidden. When travelling, staff should be encouraged to carry cash in different places and among different staff members travelling. In periods of high tension, when withdrawal, relocation or evacuation might be necessary, cash can be distributed among departing staff, partly to spread the risk and partly to ensure that staff have some cash to hand in case they become separated. Organisations should check that staff are comfortable with carrying large amounts of cash on them in situations of high tension or while travelling.

In countries where relocation or evacuation is a strong possibility, movements of cash should be prearranged and planned. The cash requirements of staff who may need to remain in place should be considered and addressed.

Case example: Sudan

In Sudan, one organisation needed to issue cash regularly as 'emergency' money for travel to local offices. To reduce the visibility and vulnerability of the cash, an amount of paper cash was placed between two sheets of paper (or a folded single sheet), and this was placed inside a special plastic pouch and laminated. Written instructions and a dotted line were printed on the paper in advance. This made a neat and protected package of pre-counted money. It also made accounting easier as there was no need to count the cash when it was issued and returned as long as the pouch was intact.

Reducing predictability

Routine increases risk, so organisations should try to avoid predictability in cash-related activities. Some common predictable risk points include:

- The monthly payroll.
- Special payments to staff prior to relocation or evacuation.
- Staff arrivals at airports and hotel/office transfers (thieves may monitor the arrival times of certain flights and may target vehicles on the main route into town).

- Trips by staff from the office to the bank and back, especially if they use the same route and travel at roughly the same time of day.
- Trips to the bank that involve more than one staff member may indicate that a larger than normal sum of money may be about to be deposited or withdrawn.

Extra security precautions can reduce predictability. For instance:

- Using an unmarked rented or local vehicle or a less obvious route to bring staff from the airport to the office or hotel.
- Changing salary periods and payment times, although this is unlikely to be popular with staff.
- Authorising a variety of staff members to go to the bank, changing routes and travel times.

Reducing vulnerability

Organisations can put in place measures to reduce vulnerability around cash, including guidelines around travelling with cash and site security measures.

To reduce vulnerability when transporting cash by road, at least two people, and preferably more than one car, can be involved. It is best to avoid predictability, and this may involve varying the number of passengers and cars used. In extreme cases, an armed escort or an armoured vehicle might be used, though this is likely to attract unwanted attention. When withdrawing cash from an ATM, a machine in a busy street with a queue of others waiting to do the same may be the most secure option. Staff should ideally withdraw money during the day and in company with a colleague to keep an eye on the surroundings. Staff may be observed taking out cash and might be followed, and so should avoid quiet streets or more dubious areas after visiting an ATM.

At the office, organisations can consider installing safes and having robust site security measures in place. Some considerations for safe security include:

- Anchoring the safe to the floor, and placing it in a back office or behind a desk so that it is hidden from visitors.
- Fitting a lock that requires two keys to open and giving the keys to two separate people, or using a key and combination lock.
- Being prepared in the event that robbers threaten violence against staff if the safe is not opened on demand (such as advising staff to hand over the keys or the combination if they are threatened).

- If a key holder is about to go away or on leave, ensure that a proper cash count is done with a new key holder, signed off by both parties.

▶ *For more information on site security, see Chapter 7.2.*

A note on identity theft

Identity theft and financial fraud, including credit card fraud, are large and growing problems. Some of the most common forms involve:

- Physical theft of cards and cheque fraud (printing fake cheques or stealing cheques).
- 'Dumpster diving' (stealing financial documents from the trash).
- Account redirection (fraudulently filling out a change-of-address form).
- Snatching a wallet or purse.
- Detaining individuals, including in their homes, while accomplices take their credit cards and PINs to a nearby ATM.

7.3.3 Cash programming

Many aid organisations have adopted cash programming as one of their main modalities for assisting people in crisis. The transfer mechanism can take various forms, such as digital transfers or vouchers, but can also involve the distribution of physical cash. The distribution mechanism should be appropriate to the context and consider practical constraints and security risks. Using banks and other financial institutions potentially reduces the security risks associated with cash transfers.

In general, when moving and storing cash for cash programming activities, many of the mitigation measures previously listed apply. Proper risk analysis, mitigation measures and monitoring are crucial. It is advisable for staff to carry out a programmatic risk assessment considering all the security risks to organisations, staff and aid recipients before and during the cash programme. Staff are not the only ones at risk when handling the cash: it is not uncommon for criminal groups to target and rob recipients of cash programmes. Cash distribution sites are also locations of high risk and will likely require appropriate site security measures.

There are also risks associated with the storage of beneficiary and financial data. Some organisations employ third-party data management tools to store and manage data. The potential data security and reputational risks associated with using such tools will need to be assessed prior to adoption.

Examples of risk mitigation in cash programming

In Afghanistan and Somalia, organisations have successfully used local remittance companies to deliver money to people in remote and insecure areas.

In Ethiopia, one international organisation took out insurance coverage against the risk of loss in transporting cash to projects in areas where there were no banks.

In Zambia, an international organisation sub-contracted delivery in remote rural areas to a bank and financial services group, which used security company vehicles to deliver the cash, accompanied by local police.

The transfer of cash on a wide scale creates institutional risks related to fraud, diversion and misappropriation. There are also compliance risks in relation to counter-terrorism legislation and donor sanctions in high-risk environments. These risks are often seen as more serious than if they were to happen with in-kind aid, and should be carefully considered, prepared for, mitigated and responded to. The reputational damage of any fraudulent activity relating to a humanitarian organisation's operations can have serious consequences (see case example below).

Case example: Turkey

In 2015, an investigation by USAID uncovered fraud involving several individuals, some working for NGOs, in cross-border humanitarian aid from Turkey to Syria. The investigation found major corruption in the procurement process, including bribery, bid rigging, kickbacks and collusion between NGO logistics staff and corrupt commercial vendors. At least one international NGO staffer faced criminal charges and extradition, and the NGOs involved suffered severe reputational damage among their donors and the broader public. The massive volume and rapidity of funding flowing to international NGOs in Turkey, which were under pressure to ramp up operations quickly, was a factor in inadequate financial controls, procurement procedures and vetting requirements.

Source: Parker, B. (2018) 'US bans aid workers in Turkey-Syria scam' The New Humanitarian, 11 September (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

Further information

Guidance, tools and discussion

Cornish, L. (2017) 'New security concerns raised for RedRose digital payment systems' Devex, 28 November (www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619).

ICRC (2021) *SAFE: Security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

International Red Cross and Red Crescent Movement (n.d.) 'CTP risk matrix template'. Module 3, Step 1, Sub-step 4, Cash in emergencies toolkit (https://cash-hub.org/guidance-and-tools/cash-in-emergencies-toolkit/all-toolkits/).

Parker, B. (2018) 'US bans aid workers in Turkey-Syria scam' The New Humanitarian, 11 September (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

The CALP Network (n.d.) Key resources (www.calpnetwork.org/key-resources/).

7.4 Criminality

In many operational settings, crime is the most prevalent security incident affecting aid personnel. This chapter discusses the range of threats posed by criminal actors – from common crime and harassment to organised crime, gang activity and the overlap with non-state armed groups – and how aid organisations can better understand and manage crime risks.

7.4.1 Types of crime and criminal environments

Crime is universal, and organisations responding to humanitarian crises will often need to contend with varying levels of criminality. While most major attacks affecting aid workers have historically been perpetrated by state militaries and non-state armed groups, in many settings criminal actors pose the greatest threat. A 2015 review found that intentional homicide rates globally exceeded deaths in conflict.[99]

Criminal activity can be driven by a number of factors, including high inequality, concentrated disadvantage and widespread unemployment. In many humanitarian contexts, crime surges as a result of political instability and where governments lack the ability to enforce the rule of law and provide meaningful economic opportunities. In many contexts, the ready supply of arms can contribute to increased violent crime. The presence of aid operations can often be a magnet and a breeding ground for corruption and crime. As well as crimes of opportunity, aid organisations can be targeted by organised crime. Criminal groups take advantage of changes in the political and economic environment to expand illegal rent-seeking.

The distinctions between criminals, conflict parties and other political and economic actors are often very blurred. Non-state armed groups and government authorities frequently collude with crime groups when interests align, and rebel movements often sustain themselves through illicit activities such as drug trafficking. However, for risk analysis and management purposes, organisations still find it useful to distinguish between economically motivated crime and the security risks stemming from armed conflict, 'acts of terror' and civil unrest.

99 Geneva Declaration Secretariat (2015) *Global burden of armed violence 2015: every body counts.* Cambridge University Press (https://doi.org/10.1017/CBO9781107707108).

Examples of economically motivated crime aid organisations need to consider in their risk assessment and mitigation strategies include:

- petty theft;
- burglary;
- extortion and bribery;
- pickpocketing and bag-snatching;
- mugging;
- armed robbery;
- intimidation and extortion;
- carjacking and vehicle theft; and
- kidnap for ransom, including 'express kidnappings', where victims are held just long enough to force them to withdraw funds with their bank card.

Most of the crimes listed above involve violence or risk becoming violent. It is also important to remember that working in a high-crime context, where insecurity is pervasive, can have a severe impact on an individual's stress levels and overall wellbeing. This is compounded when staff are from the country, and the risks in the environment also affect their family.

'White-collar' crimes such as embezzlement and fraud are also common, though less directly relevant to duty of care and physical security risk management (although they can have knock-on effects that can result in security risks) and tend to be under the purview of an organisation's financial, legal and compliance teams.

► *To learn more about abduction, see Chapter 7.9.*

► *For more details on risks in the digital sphere, see Chapter 6.2.*

The presence of organised groups seeking to exert control over local areas and inhabitants adds another layer of risk. The risk of harassment and extortion can be especially difficult to mitigate as targeting is persistent rather than opportunistic, and organisations may find themselves subject to repeated harassment, intimidation and extortion. Gang culture, social norms and desire for status within the group often create an environment where violence is expected and rewarded. The threat to aid actors working in these contexts requires significant attention and robust security risk management measures.

7.4.2 Practical considerations

Good practice in security risk management requires developing an understanding of the context and crime risks, followed by measures to mitigate those risks and deter prospective offenders. Measures include increased physical protection of assets and overall site security to prevent theft and break-ins, and staff guidance on how to reduce exposure to crime risks. Some organisations have invested in programming that tackles crime and violence, as a way of reducing the risks to the community as a whole.

Contextual understanding

Similar to conflict-related insecurity, comprehensive and up-to-date context analyses, risk assessments and actor mapping are crucial tools for managing the risks of crime.

Understanding the context involves identifying whether the risk stems from crime that is organised, opportunistic or a combination of the two. Organised crime is complex and often connected to wider political and economic interests, as opposed to opportunistic, 'common' or 'street' crime, which is more sporadic and situational.

Crime rates are generally higher in urban than in rural areas, and violent crimes tend to cluster in specific areas within cities and even neighbourhoods.[100] There is typically a high degree of spatial and demographic clustering for many types of violent and non-violent crime. As urban violence is itself increasingly creating humanitarian crises and more humanitarian action is taking place in urban areas, context analysis, key actor mapping and basic assessment of criminal groups – who, what, where, when and how – should all be part of the risk assessment.

The density and complexity of urban environments mean that security dynamics may differ across a large number of small areas in close proximity to each other, requiring more granular risk assessments than may be needed for rural areas. Several humanitarian organisations in Latin America and the Caribbean maintain active mapping of gangs and the territories they control, using local informants to keep information up to date. Lines can change daily, even shifting by street.

Organisations benefit from identifying reliable sources of information within the community or among other local actors. For example, organised criminal groups

100 See Muggah, R., Aguirre, K. and Chainey, S. (2017) 'Targeting "hot spots" could drastically reduce Latin America's murder rate' *Americas Quarterly* (https://americasquarterly.org/article/targeting-hot-spots-could-drastically-reduce-latin-americas-murder-rate/).

may transport, deliver and distribute items in defined locations and at set times. With the help of local communities, it is possible to know when activities usually take place, and so avoid those times and places.

Organisations should also assess how their presence and programming impact criminal economies; it is not enough to assume that, if they do not directly interfere with their interests, criminal actors will respond in kind. In areas of high violent crime, 'crime-sensitivity' needs to join conflict-sensitivity among an organisation's competencies and approaches.

▶ *See Chapter 4.1 for details on how to carry out analyses and assessments.*

Risk mitigation measures

In addition to carrying out a risk assessment and other efforts to better understand the context, organisations might consider some of the examples of practical risk mitigation measures presented in Table 22.

Table 22 Practical measures to deter, prevent and mitigate criminal risks

Measure	Description	Notes
Asset management and remote working	• Maintain an up-to-date inventory of assets and implement tracking systems for high-value items. • Conduct regular audits. • Have protocols in place for remote working.	As working from home has become more commonplace, so organisations have needed to introduce procedures covering how computer equipment and other work materials are transported and kept. Simple measures, such as not transporting computers in computer bags, can significantly lower the risk.

Measure	Description	Notes
Reporting incidents	• Ensure robust incident reporting – even for minor incidents.	Seemingly minor criminal incidents can have severe consequences. The theft of a phone, computer or bag containing personal or financial information can provide larger criminal opportunities. Seemingly minor criminal incidents can have severe consequences. The theft of a phone, computer or bag containing personal or financial information can provide larger criminal opportunities. Appropriately reporting all cases, and analysing them properly, can support response and future prevention measures. *See Chapter 4.4 for more on incident reporting.*
Physical security measures, including access control	• Take anti-robbery and anti-theft measures in all offices and project facilities, even those only accessible to organisation staff. • Install physical security measures such as fences, locks, alarms and CCTV, as appropriate. Conduct regular maintenance checks. • Employ strict access control measures (e.g. ID badges and visitor logs) in offices, warehouses and distribution sites.	*For more details, see Chapter 7.2 on site security.*

Measure	Description	Notes
Cash handling procedures	• Establish secure cash handling procedures, including using banks or secure transfer methods where possible. – Minimise cash transactions. – Avoid routines related to payments. – Maintain confidentiality of information.	*See Chapter 7.3 on cash security for more details.*
Personal safety measures	• Promote personal safety measures for staff, such as maintaining a vigilant attitude and awareness of surroundings, avoiding high-risk areas and times, avoiding predictable routines and travel routes, keeping items secure and out of sight and reach, avoiding displays of wealth and using buddy systems.	All guidance needs to be context-specific, kept regularly updated and shared with staff. For instance, in one context staff may be advised never to carry cash or valuables on their person, while in another they may be at greater personal risk if they do not have something to hand over to a robber.
Liaison with authorities	• Maintain regular contact with local law enforcement and other authorities.	Share information and seek support when needed and if appropriate. Note, however, that some authorities may not be reliable sources of information and protection in environments where state and criminal actors are enmeshed.
Anti-corruption measures	• Implement and enforce anti-corruption policies, including vetting of staff and vendors. • Conduct regular audits and awareness training.	–
Incident management	• Be prepared to respond to an incident, providing immediate support to affected individuals as well as long-term care.	*See Chapter 4.4 for more details on responding to incidents.*

Measure	Description	Notes
Staff care	• Consider and develop staff care structures and interventions. • Provide psychosocial support in the aftermath of an incident as well as more regularly for staff to manage stress.	Living in high crime environments can have similar stresses and negative psychological impacts on staff and their families as working in conflict settings. Being the victim of violent crime can cause long-lasting physical and psychological trauma. *See Chapter 5.4 on staff care.*
Digital security measures	• Crime is increasingly perpetrated online, via social media and other digital communication means. • Implement digital security measures, including guidance for staff on how to keep themselves safe online.	For example, depending on privacy settings, what staff post on social media can be used by criminal actors to identify and target victims. *See Chapter 6.2 on digital security.*

Harassment

The risk of harassment by criminal actors and others is a significant threat to aid workers. Harassment is abusive behaviour that might be physical or verbal, and might take place in person, for instance at checkpoints or during distributions, or online. Most harassment cases are verbal events – usually, physical harassment comes after a prior incident of verbal harassment. It can happen for a variety of reasons; it may be a tactic used by criminals to place staff under pressure to comply with demands, or community members may harass staff due to perceptions about the work their organisation is doing. Incidents should always be reported, not least because they can lead to more serious threats.

Several measures can help reduce the risk of harassment:

- Monitoring local sentiment towards the organisation and its staff, including on social media.

- Training staff on how to conduct themselves in a way that does not draw negative attention, such as respecting and adapting to local customs, discussing the organisation's activities and mission, and avoiding discussions on local politics or culture.
- Ensuring staff follow security protocols, such as travel guidance, avoiding large crowds or charged environments, carrying correct documentation, maintaining a safe online presence and reporting incidents.
- Training staff on situational awareness, including suspicious individuals and situations that might escalate.
- Training staff on how to respond to different types of harassment (e.g. removing themselves from a situation and on to a safer place, calling for help or attracting attention).

Following an incident, organisations can discuss with relevant stakeholders why the harassment took place and how to avoid future incidents. Additional measures, such as suspension of activities or changes in staff movements, may be required. Affected staff may also require post-incident care.

Beyond protective measures: negotiation

Just as with other security threats, organisations need to be aware of the criminal threat in the environments where they work and understand how their own presence and programming potentially interact with and affect crime dynamics. While aid organisations have developed tools for mapping, outreach and negotiation with armed groups and political power holders, they rarely take a similarly proactive approach with criminal actors.

Humanitarian organisations tend to avoid engaging with criminal groups because of the legal, ethical and reputational risks such engagement may entail – not to mention security risks for the organisation in becoming a known entity to a group that may decide to target it or its staff. Engaging in negotiations with these actors could be seen as complicity, and could potentially lead to legal challenges. There is no legal framework similar to the Geneva Conventions to provide a principled basis and guide for organisations to engage with criminal actors as they would with conflict parties. It can also be difficult to identify who to contact, and who has the authority to represent the group.

Some aid organisations have had success in negotiating access with criminal actors by adopting lessons and practices from community development groups that work to decrease violence at the grassroots level.

Negotiations with criminal groups can be patterned after those with non-state armed groups, aimed at achieving concrete objectives such as security assurances for certain programme activities or access to locations that criminal groups control. As with conflict actors, this can often best be achieved not through appealing to abstract humanitarian principles or ethics, but by identifying an interest held by the criminal group that aligns with humanitarian objectives. If criminal actors are local to the area, they may have children or other family members and social ties to the community that would benefit from the aid programming. They may also have an interest in being seen and treated as the controlling authority.

Case example: Operating in Haiti amid gang control

An international NGO running health facilities in Haiti continually communicated and negotiated with gang leaders, community members, police and other authorities, emphasising the importance of protecting health workers and facilities so they can be available to treat everyone, including injured gang members. The organisation also maintained a confidential agreement with the police covering entry into the organisation's facilities.

Programmatic approaches to crime risk management

In addition to direct negotiation, aid organisations have engaged in community-level programmatic interventions aimed at reducing crime and violence. For example, organisations working in Latin America and the Caribbean have implemented projects focused on crime reduction and alternatives for at-risk youth.[101] Such approaches require highly localised, even street-by-street analysis and outreach measures.

101 See, for example, Cure Violence Global, which applies a public health methodology to tackle violence: https://cvg.org/about/

Further information

Research and discussion

Geneva Declaration Secretariat (2015) *Global burden of armed violence 2015: Every body counts.* Cambridge University Press (https://doi.org/10.1017/CBO9781107707108).

GISF (2023) *Good practices, lessons learned, and the unique challenges affecting security risk management in urban humanitarian responses* (https://gisf.ngo/resource/good-practices-lessons-learned-and-the-unique-challenges-affecting-security-risk-management-in-urban-humanitarian-responses/).

Humanitarian Outcomes (2021) *Aid worker security report 2021. Crime risks and responses in humanitarian operations* (https://humanitarianoutcomes.org/AWSR2021).

ICRC (2023) 'Organized Crime, IRRC 923', June (https://international-review.icrc.org/reviews/irrc-no-923-organized-crime).

Lucchi, E. (2013) *Humanitarian interventions in situations of urban violence.* ALNAP (www.urban-response.org/system/files/content/resource/files/main/alnap-lessons-paper-urban-violence.pdf).

Mohor, D. (2023) 'Gang violence in Latin America poses a challenge for the aid sector' The New Humanitarian, 17 May (www.thenewhumanitarian.org/analysis/2023/05/17/gang-violence-latin-america-challenge-aid-sector).

Muggah, R. (2017) 'A humanitarian response to Central America's fragile cities. The humanitarian consequences of violence in Central America' *Humanitarian Exchange* 69. Humanitarian Practice Network (HPN) (https://odihpn.org/publication/humanitarian-response-central-americas-fragile-cities/).

Muggah, R., Aguirre, K. and Chainey, S. (2017). 'Targeting "hot spots" could drastically reduce Latin America's murder rate' *Americas Quarterly*, 9 March (https://americasquarterly.org/article/targeting-hot-spots-could-drastically-reduce-latin-americas-murder-rate/).

Savage, K. and Muggah, R. (2012) *Urban violence and humanitarian action: Engaging the fragile city.* ALNAP (https://library.alnap.org/help-library/urban-violence-and-humanitarian-action-engaging-the-fragile-city).

Resources

Cure Violence Global (n.d.) 'About Cure Violence Global'. Webpage (https://cvg.org/about/).

Davis, J. et al. (2020) 'Module 2: Actor mapping and context analysis' in *Security to go: a risk management toolkit for humanitarian aid agencies*, 4th edition. GISF (www.gisf.ngo/resource/security-to-go/).

Igarapé Institute (n.d.a) *Humanitarian action in situations other than war* (HASOW) (https://igarape.org.br/en/hasow/).

Igarapé Institute (n.d.b) 'Homicide monitor' (https://homicide.igarape.org.br/).

7.5 Hostile surveillance

Hostile surveillance can present a significant security risk to humanitarian workers and vulnerable populations. It can however be overlooked in standard humanitarian security risk management efforts because it is often an 'invisible' risk. Drawing on the expertise and experiences of human rights and social justice workers, for whom this is a persistent concern, this chapter looks at hostile surveillance, its implications for humanitarian work and responses to it, including surveillance detection and anti-surveillance measures.

7.5.1 Understanding hostile surveillance

While 'surveillance' involves systematic monitoring to gather information or exert control, 'hostile surveillance' specifically targets individuals, assets or properties with pre-attack planning or malicious intent. Note that not all surveillance is covert – sometimes it is meant to be visible (e.g. as a form of intimidation).

Table 23 Distinction between surveillance and hostile surveillance

Surveillance	Hostile surveillance
• Surveillance can be conducted by various entities, including governments and private companies, for purposes such as security, intelligence gathering or monitoring. • Surveillance may serve legitimate purposes like public safety or law enforcement but can also be used nefariously, violating privacy or suppressing dissent. • Examples include government monitoring of communications, social media tracking, and corporate surveillance for market research.	• Hostile surveillance is conducted with hostile intent, directly threatening the safety and security of targets. • It aims to gather intelligence, identify vulnerabilities, or plan and execute hostile actions like theft, espionage or physical attacks. • Stalking, reconnaissance activities, the use of spyware technologies, and monitoring of security measures to identify weaknesses to be exploited are typical behaviours associated with hostile surveillance.

Hostile surveillance in a humanitarian setting can be conducted by various actors, including non-state armed groups, government forces and criminal elements (see the box below).

Possible surveillance actors

- Non-state armed groups may conduct hostile surveillance to gather intelligence, monitor humanitarian activities and target aid workers.
- In conflict-affected regions, government forces or security agencies may engage in surveillance of humanitarian organisations in an attempt to track possible infiltration of non-state armed groups in the local population.
- Criminal elements may conduct surveillance to exploit or disrupt humanitarian operations for financial gain or to further their interests.

Organisations should be mindful that state intelligence agencies may conduct surveillance on humanitarian actors and that this intelligence-gathering can influence how other national government actors perceive and engage with these organisations. Regions experiencing armed conflict or humanitarian crises are especially susceptible to such surveillance.

7.5.2 Types of hostile surveillance

This section presents common types of hostile surveillance and the tactics associated with each. These tactics may be used individually or in combination.

Physical surveillance

- **Stakeouts:** Individuals or groups may conduct stakeouts to observe and monitor the movements of their targets from a concealed location.
- **Shadowing:** Hostile actors may follow their targets closely, sometimes on foot, to gather information about their routines, activities or vulnerabilities.

Technical surveillance

- **Electronic eavesdropping:** Hostile actors may use listening devices, bugs or wiretaps to intercept and monitor communications, including phone conversations, emails and electronic messages.

- **Video surveillance:** Cameras and recording devices are deployed to monitor targets' activities, movements and interactions in various locations, such as residential spaces workplaces or public spaces.
- **GPS tracking:** Global positioning system tracking devices may be covertly installed on vehicles or personal belongings to monitor targets' movements and gather location data.
- **Unmanned aerial vehicles (UAVs) and satellites:** Advanced technologies such as UAVs (drones) offer aerial surveillance capabilities, allowing hostile actors to conduct reconnaissance and monitor activities from a distance. Satellites provide wide-ranging surveillance coverage, offering high-resolution imagery and real-time monitoring of large geographic areas.

Cyber surveillance

- **Hacking and malware:** Hostile actors may use hacking techniques, malware/spyware or phishing attacks to gain unauthorised access to targets' devices, networks or online accounts, allowing them to monitor activities, steal sensitive information and contacts, or disrupt operations.
- **Social engineering:** Hostile actors manipulate individuals or employees through deception or psychological tactics to extract information or gain access to sensitive data, passwords or systems.
- **Data mining and open-source intelligence:** Hostile actors may collect information from publicly available sources, social media platforms or online databases to gather intelligence about targets, their affiliations or vulnerabilities.

▶ *See Chapter 6.2 on digital security considerations.*

Covert observation

- **Disguises and cover identities:** Hostile actors may adopt disguises or create false identities to blend in with their surroundings, or to 'engage' with targets surreptitiously, to conduct covert surveillance without arousing suspicion.
- **Espionage and undercover operations:** This involves infiltrating target organisations, groups or communities to gather intelligence, establish relationships or gain access to restricted areas or information.

Case example: Yemen

In Yemen, aid workers have experienced surveillance from local government actors as well as international groups. Following project visits, target communities are known to have been approached and asked about the organisation and its staff. This affects how the target communities view the organisation and can undermine local perceptions.

7.5.3 Risks associated with hostile surveillance

The risks associated with hostile surveillance in humanitarian assistance extend beyond immediate security concerns. At its core, risk in this context pertains to the uncertainty surrounding the safety and efficacy of aid delivery, encompassing threats to personnel, resources and the integrity of humanitarian operations. Hostile surveillance amplifies these risks by introducing the potential for compromised confidentiality, targeted attacks and operational disruptions.

For example, intercepted communications or compromised data systems may expose the local population and communities to reprisals from hostile actors. Similarly, aid workers operating in environments where hostile surveillance is prevalent may face increased risks of physical harm, abduction or harassment.

A perception of humanitarian organisations as legitimate targets for surveillance or attack may also deter individuals from seeking assistance or cooperating with humanitarian initiatives, further exacerbating vulnerabilities and hindering access to essential services.

7.5.4 How to respond to hostile surveillance

Humanitarian actors can effectively respond to hostile surveillance tactics by being aware and having preventive measures in place. This can be achieved by assessing the surveillance risks, training staff on preventive measures and implementing surveillance detection and anti-surveillance strategies. Surveillance detection involves vigilant observation and monitoring of the surrounding environment to identify potential threats or suspicious activities

before they escalate into security breaches. Anti-surveillance measures focus on countering and deterring hostile surveillance efforts.

Anti-surveillance and counter-surveillance

There are distinctions between anti-surveillance and counter-surveillance, with the latter being beyond the scope of this book and typically utilised by military and law enforcement with specialised training and skills. Counter-surveillance is reactive and aggressive, whereas anti-surveillance is a preventive measure. Anti-surveillance involves simpler tactics, such as varying routines and routes, deploying physical security measures like surveillance cameras and personnel, and fostering community relationships for additional support in detecting and responding to surveillance. Rather than relying on extensive security measures or force, anti-surveillance can be integrated into an organisation's acceptance approach, emphasising regular interaction and communication with local communities.

An initial starting point can be a conversation with security staff or local/regional experts who understand the threats and risks of surveillance relating to the location, the profile of staff or the programme. This can be followed by a comprehensive risk assessment. Once the surveillance risks are identified, organisations can train their staff and put preventive measures in place.

► *See Chapter 4.1 for more information on how to carry out a risk assessment.*

Human rights defenders and activists frequently use a combination of the following anti-surveillance techniques depending on the context; some of these can also be utilised by humanitarian organisations to detect and thwart hostile surveillance.

Table 24 Example risk mitigation techniques

Technique	Details
Pattern recognition	Establishing baseline patterns of normal behaviour and activities within the organisation's premises or programme/project sites allows for the detection of anomalies or deviations that may indicate surveillance activities.
Route analysis	Regularly varying routes and schedules for humanitarian operations and personnel minimises predictability and reduces the likelihood of being targeted for surveillance.
Behavioural observation	Training staff to observe and report suspicious behaviours or individuals, such as people loitering or exhibiting unusual interest in organisational activities, may help in early detection of potential threats.
Technical surveillance counter-measures	Utilising electronic detection equipment to sweep for hidden surveillance devices or signals within the organisation's premises helps identify covert surveillance attempts.
Communication monitoring	Monitoring communication channels for unusual or unauthorised activities, such as unauthorised access attempts or unusual network traffic, can help detect electronic surveillance attempts.
Digital communication hygiene and device protection	Avoiding open wifi networks, using VPNs and a password manager, refraining from sharing sensitive personal information on WhatsApp and other insecure communication platforms, fact-checking information before sharing, and staying vigilant against misinformation.
Data minimisation	Taking measures to reduce the amount of data individuals have on their devices which could be used against them in the event of a breach, such as dating apps, social media/online profiles and banking details.
Operational security	Implementing strict operational security measures, such as limiting the dissemination of sensitive information and employing need-to-know principles.
Collaborative partnerships	Forging robust collaborations with experts in counter-surveillance as well as social justice/human rights organisations, leveraging their expertise to tackle the risk of hostile surveillance.

Mitigation measures can be incorporated into the security plan to address identified surveillance risks, and training can be built around them to enable staff to actively contribute to surveillance detection efforts. Relevant staff should be made aware of and receive regular training on surveillance threats, detection techniques and reporting procedures. It is worth noting that hostile surveillance awareness is typically absent from standard HEAT courses; integrating the fundamentals of surveillance awareness into these would be highly beneficial.

Managing the risk of hostile surveillance in humanitarian assistance demands a multifaceted approach that encompasses surveillance detection and anti-surveillance strategies tailored to the sector's specific challenges. To respond to hostile surveillance, humanitarian actors can implement a range of strategies, including pattern recognition, route analysis, behavioural observation, technical surveillance counter-measures, communication monitoring and operational security measures. Fostering a culture of surveillance awareness through regular training sessions and awareness-raising helps staff actively contribute to surveillance detection efforts. Collaborative partnerships with experts in counter-surveillance and social justice/human rights organisations can further enhance the effectiveness of anti-surveillance measures.

Further information

Surveillance resources

Haggerty, K.D. and Gazso, A. (2005) 'Seeing beyond the ruins: surveillance as a response to terrorist threats' *The Canadian Journal of Sociology* (https://doi.org/10.2307/4146129).

McCue, C. (2007) 'Surveillance detection – an overview' in *Data mining and predictive analysis* (www.sciencedirect.com/topics/computer-science/surveillance-detection).

7.6 Civil unrest

Protests, demonstrations, riots and other mass gatherings or disruption – as well as the authorities' response to them and any criminality or extortion that ensues – can pose a risk to people, property and humanitarian operations. In any operational context, but especially in tense and contested settings, civil unrest can erupt suddenly and may involve or turn into violence and aggression. Violence can break out spontaneously, or it might be planned and instigated. Planned, peaceful gatherings such as political events or protests can devolve unexpectedly into civil unrest. Equally, long-simmering tensions can suddenly erupt into violence following a trigger event. Aid organisations can also face risks from unruly crowds, even mob violence, in programme settings such as distribution sites and displacement camps. This chapter covers some of the potential mitigation measures for these risks, including situational awareness, preparation (SOPs and contingency plans), and training and awareness of potential courses of action.

7.6.1 Situational monitoring and analysis

While challenging to predict and track, it is important that civil unrest and its different manifestations form part of risk analysis and regular monitoring efforts.

- **While not all can be predicted, it can be useful to identify potential triggers.** Examples include: political and economic changes such as a decision by a foreign power to intervene militarily; a sudden economic crisis brought on by international trade conditions; a government decision to cut subsidies on essentials such as food or fuel; a decision to close a refugee camp before people are willing to go home; the arrest or assassination of a prominent figure; aid distributions; and national/local elections.
- **Growing tension and frustration can often be detected in advance.** Close monitoring of local media and sentiment is important, and if possible, should be a designated responsibility of a staff member or unit. This could include tracking local news and social media, maintaining contact with local communities and leadership and testing levels of acceptance.
- **Context analysis can help predict possible responses to civil unrest.** The legal context and how past events unfolded can help predict how local authorities and others may respond to demonstrations and other gatherings. These can feed into planning and preparedness measures.

Case example: Non-violent responses to civil unrest can still pose a risk to operations

Violence is not the only risk that aid organisation staff face during periods of civil unrest. One such example occurred during the 2018 election season in the Democratic Republic of Congo, where the authorities shut off internet and SMS services nationwide for 20 days, with implications for aid operations and security risk management.

Organisations might consider the following questions as part of their monitoring and analysis.

- Have there been episodes of civil unrest in the past? If so, where did they start, and how did they evolve? Is there a pattern that could repeat itself? What were the main causes? What level of violence was involved? Who or what was the target of that violence?
- What factors can trigger civil unrest? What form might any violence take? How have authorities previously responded to episodes of unrest?
- Who are the targets of local resentment and what is the root cause of this tension?
- Are the organisation or its staff vulnerable to the risk of civil unrest? How can vulnerabilities be mitigated?
- Are some staff at more risk than others, considering their personal risk profile?
- Are specific projects or types of intervention at risk, for example projects deemed to be at odds with the local culture or religion, or perceived as supporting one warring party or another?
- How do the authorities respond to civil unrest at national, local and community level? Gas? Water cannon? Rubber bullets?
- How do religious or ethnic authorities respond to civil unrest (indigenous law and practices)?

Relating to the organisation's own activities and programmes, questions to consider include:

- What expectations do local inhabitants have?
- Are they expecting something from the organisation, e.g. a distribution?
- Can the organisation manage expectations through clear communication prior to any programmatic activity?

Case example: UN staff killed in an unrelated protest in Afghanistan

An organisation in proximity to civil unrest can be at risk of violence even when it is not the direct target, as this example involving the UN shows. In 2011 there were protests in northern Afghanistan in response to the burning of a Qur'an by a US pastor in Florida. The protest was planned but violence spread spontaneously and was unforeseen. When protesters breached the UN compound guards opened fire. Four guards, three UN staff members and five protesters were killed.

7.6.2 Planning and preparedness

Planning and preparedness measures might include the following:

- **SOPs and contingency plans.** Plans and procedures should cover all possible events that could become violent (planned protests, election rallies, social and community events, aid distributions and any other large gatherings) and their consequences (government restrictions, theft, looting and other forms of violence). Each office will likely require its own security procedures and protocols, including contingency plans (hibernation, evacuation and relocation plans); up-to-date contact lists (available to all staff); up-to-date contact lists for medical emergencies (hospitals and air charter companies for example); and information security protocols (regular computer backups and marked files/documents to be destroyed and taken in case of evacuation, for example). Once plans have been developed, staff must be informed and trained on procedures and expectations.

- **Taking protective measures.** Measures should directly refer to the risks and threats identified. Safe rooms could be designated and prepared in each building, with hibernation kits, communication equipment, first aid kits and fire extinguishers. In the event of power outages or interruption of communication services, power and communication backup systems should be available in all of the organisation's buildings.

▶ *See Chapter 7.2 on site security.*

- **Movement management.** If civil unrest is imminent, the organisation can consider alternative work modalities for its staff, such as working from home, reducing staff numbers or movement restrictions. Consideration should also be given to when and where crowds are likely to gather and where they will move to (via which route). In the case of a political rally routes may be clearly identified. In the case of a distribution, this would include well-managed entrance and exit routes for aid recipients and staff, as well as setting up first aid response areas.
- **Incident and crisis management response.** The organisation should be prepared to quickly respond in the event of a critical incident, or if civil unrest triggers an organisational crisis management response.

▶ *See Chapter 4.4 for more on incident response and crisis management.*

- **Training on key actions that staff can take to keep themselves and their colleagues safe.** Staff are, of course, entitled to participate in gatherings and exert their rights as citizens, and organisations can provide training to ensure that, if these events become dangerous, staff know how to keep themselves safe. This training could cover knowledge and awareness of security rules and procedures, especially around high-risk events or locations, how to respond to crowd control weapons such as rubber bullets, clubs and tear gas, and guidance on how to seek safety and shelter. Staff must be made aware that their safety takes priority over the organisation's equipment, premises or stores. If possible, valuable equipment such as laptops should be removed and equipment that cannot be removed could be disabled (e.g. vehicles). Sensitive equipment that cannot be removed or disabled may need to be destroyed.
- **Visibility.** Staff should consider their organisational visibility. If an organisation has good local acceptance and is not directly targeted, it may be protected from crowds if it is clearly visible and identifiable. However, if an organisation is a focus of dissatisfaction, or is not well known locally, it would be better to remove office and vehicle signage and for staff to adopt a low profile.

▶ *See Chapter 4.2 for more on acceptance measures.*

Guidance during elections

Know the context

What is the political system and electoral process? Who are the candidates and what is their political agenda? What is the election calendar?

Know the different stages of the election period and associated risks

The stages can often be broken down into pre-election/campaigning, polling/voting, vote counting and results declaration, the installation of a winner and accompanying celebrations/protests.

Each of these stages can vary in duration from a day to months. Associated risks include online incitements to violence; acts of violence or riots near polling stations or during mass gatherings; escalation and perpetuation of ethnic or sectarian violence; clashes between groups; theft, vandalism and physical attacks on property; and intimidation and harassment of individuals, groups and organisations. Authorities may impose curfews and movement restrictions, curtail the media, shut down services/utilities (e.g. internet and electricity) and detain organisational staff. Political groups have been known to confiscate organisational assets for electoral purposes.

Implement mitigation measures

Mitigation measures can include:

- Travel management protocols, including movement restrictions and curfews (especially around high-risk areas and during particular election stages).
- Guidance for staff on how to stay safe when voting (such as not travelling alone and being situationally aware).

- Securing buildings and vehicles; preparing staff on how to respond to incidents of theft, harassment, intimidation and detention and an increased number of checkpoints and roadblocks.
- Adapting ways of working during election periods (e.g. remote working).
- Guidance for staff on how to keep themselves safe in heated political climates (e.g. avoiding political discussions (in person and online), not wearing colours that could be affiliated with a political party and keeping an eye out for groups and discussions that could turn violent).

Staff can be trained on how to liaise with political parties and authorities in the event they ask for support or services.

7.6.3 During an episode of civil unrest

If civil unrest breaks out before the organisation has had time to take mitigation measures, or if those measures fail, it is imperative that staff monitor the situation closely and are prepared to take immediate action. This might include the following:

- **Implementing contingency plans.** For example, if protesters or rioters enter a building, staff immediately take shelter in a safe room.
- **Reconsidering modes of transport and restricting travel, particularly in risky areas.** For example, it may be safer to travel in nondescript local vehicles or taxis than in large, conspicuous vehicles.
- **Considering whether to request support from the authorities/security forces.** Security forces will likely be armed and this needs to be balanced against organisational policy and the level of risk, especially if security actors are involved in controlling or dispersing crowds.
- **Ensuring that communication between staff is maintained.**
- **Potentially opening up channels of communication with protest leaders.** All negotiations should ideally be conducted by staff who have received training in this area.

Case example: Humanitarian organisations attacked during communal violence

In 2014, mobs attacked the offices and residences of several humanitarian organisations in Myanmar. The attacks were fuelled by tensions between two religious groups. Several offices and buildings were entered, and furniture and equipment were destroyed. Following the incident humanitarian staff were relocated from their offices, disrupting operations. The incident shows how disputes can quickly spiral, creating risks for aid organisations in the area. Better monitoring of the local context could have identified likely risks ahead of the incident, giving organisations more time to prepare staff and facilities.

7.6.4 After an episode of civil unrest

Following an incident, organisations may wish to:

- Consider the working modalities of staff – it may be better for them to keep working from home and to maintain a low profile while things settle down.
- Maintain heightened security measures until the situation has clearly calmed down and there is no perceived risk of further threat or retaliation.
- Consider the impact of the event on affected staff and provide support as required – be prepared to support staff who have relocated or been evacuated.
- Consider the organisation's public relations position and what messages, if any, the organisation issues – a constant review of public sentiment and the organisation's outreach efforts is beneficial.
- Be prepared to face hostile surveillance in the aftermath of a serious event linked to the organisation.
- Consider a review of the organisation's decision-making and actions – learning lessons from past events plays a critical role in improving an organisation's safety and security risk management system and programmatic approach (e.g. how distributions are conducted).

Further information

Resources

International Foundation for Electoral Systems (IFES) (n.d.) ElectionGuide (www.electionguide.org/elections).

Overseas Security Advisory Council (OSAC) (2019) *Surviving a protest* (www.osac.gov/Content/Report/0b882e6f-c05f-4d1c-9601-15f4ad6883fc).

OSAC (2022) *Preparing for election violence* (www.osac.gov/Content/Report/d7cd68ad-cee9-4386-b647-1e9f5c7745f6).

OSAC (2023) *Coups d'état: thinking through your organization's response* (www.osac.gov/Content/Report/cf60640f-7c0b-4410-ae6f-228341955588).

7.7 Sexual violence

Sexual violence is one of the most serious incidents that aid workers can face and may have lifelong consequences for survivors. Aid organisations have a duty of care to protect their staff from threats of this nature, whether they emanate from within or outside the organisation. While the role security staff play in managing this type of incident will vary by organisation and will likely have to be managed in collaboration with other colleagues (particularly HR and other specialist staff), security risk management can play an important role in preventing, preparing for and responding to incidents. This chapter presents key definitions and actions for security professionals to consider, including how to take a survivor-centred approach when responding to this type of incident.

7.7.1 Definitions and scope

Sexual violence is any act of a sexual nature, or attempt to obtain a sexual act, that is unwanted or forced. Sexual violence can be perpetrated by any individual against another (regardless of their relationship) using physical force, coercion or threats. Sexual violence includes scenarios in which offenders exploit an environment that is coercive, or an individual's inability to provide authentic consent.[102]

The line between sexual harassment and coercion or assault can sometimes be hard to draw, but it is important to understand that these incidents often co-occur and can be seen as existing along a continuum that covers acts from minor (e.g. sexual comments) to severe (e.g. rape).[103] See Figure 12.

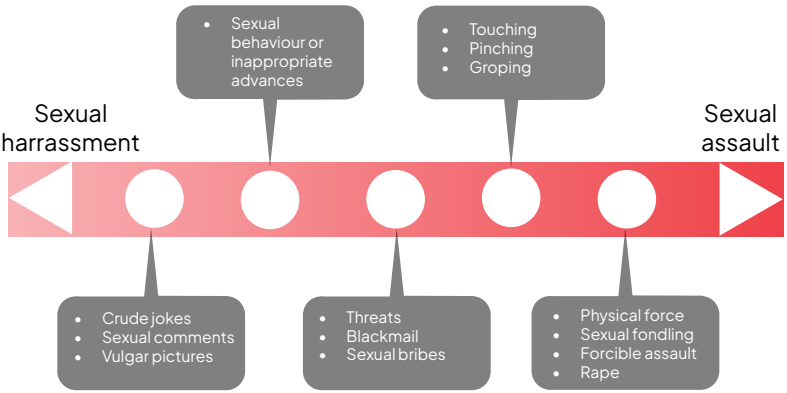
Within the context of the aid sector, sexual violence can take many different forms, for example:

- individual targeting, including the administration of drugs to incapacitate the target;
- sexual abuse and exploitation, where aid workers are coerced by individuals in positions of power (including other aid workers); and
- as a weapon of war or intimidation, where aid workers are targeted by armed actors.

102 EISF (2019) *Managing sexual violence against aid workers: prevention, preparedness, response and aftercare* (https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/), pp. 12–13.

103 EISF (2019) provides a full list of forms of sexual violence and their definitions.

Figure 12 Examples in the continuum



Source: EISF (2019) M*anaging sexual violence against aid workers: prevention, preparedness, response and aftercare* (https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/).

A note on gender-based violence

Gender-based violence is an 'umbrella term for any harmful act that is perpetrated against a person's will, and that is based on socially ascribed (gender) differences between males and females'.[i] It encompasses various forms of violence, including but not limited to sexual violence. This chapter focuses specifically on incidents of a sexual nature – from harassment to assault – given their extreme nature and the role security professionals play in mitigating these risks. All forms of gender-based violence should be considered and addressed within an organisation, as these can be precursors to or accompany sexual violence.

i IASC (2015) *Guidelines for integrating gender-based violence interventions in humanitarian action* (https://gbvguidelines.org/en/gbv-guidelines/).

Working in violent environments where there is weak rule of law can increase the risk of particularly traumatic forms of sexual violence. Staff may also experience sexual violence in domestic settings, and organisations should discuss internally how and under what circumstances they may respond to these types of events in order to ensure the wellbeing of the affected staff member.

Unlike other critical incidents within the aid sector, risk management for sexual violence is still hindered by stigma as well as misconceptions around what it is and why it happens (e.g. that it only happens to women, most perpetrators are strangers, it is consensual if there was no physical resistance, it is always extremely violent, and survivors report immediately after an incident occurs). It is imperative that staff involved in managing incidents of this nature are trained and can access support from experts.

Related terms and areas of work

The following terms and areas of work have similarities and are worth defining with more clarity.

Protection from sexual exploitation and abuse (PSEA) is an area of work that focuses on protecting affected populations from sexual exploitation and abuse within humanitarian response operations. For further details, see: https://psea.interagencystandingcommittee.org/

Safeguarding encompasses efforts to protect everyone (including staff, volunteers and aid recipients) from all forms of harm, abuse and exploitation. To learn more, see: https://safeguardingsupporthub.org/

Conceptually, sexual violence affecting aid workers and PSEA fall within safeguarding, although the definitions and the way these workstreams interact in practice can differ across organisations. The important point is that these areas of work collaborate and support each other where appropriate.

7.7.2 Risk considerations

Risk considerations relating to sexual violence can be grouped under four areas:

- individual risk considerations;
- perpetrator profiles;
- organisational risk factors; and
- external risk factors.

Strategies for risk mitigation should aim to address all four areas. Security staff can ensure that procedures prioritise not only managing staff behaviour, but also deterring potential perpetrators and addressing other risk factors. For example, organisations can focus on training staff on how to reduce their exposure to the risk, while also putting in place measures to deter perpetrators, addressing the organisational and external conditions that contribute to sexual violence (when possible) and mitigating risks in these environments.

Individual risk considerations

While certain profiles are at particular risk of sexual violence, sexual violence can affect anyone, and preparedness and response measures must account for this. An individual's intersectional identity can affect their vulnerability to sexual violence, including gender, race, sexual orientation, disability and relative power and choice. National aid workers are at particularly high risk, especially in violent environments or patriarchal societies. These staff members are also often afforded fewer safeguards than their international counterparts, for example support while travelling to and from work.[104] A survey for the UN has found that 'non-staff' (such as consultants, interns and volunteers) are also particularly vulnerable and are less likely to feel able to report incidents.[105]

Under-reporting of sexual violence incidents is pervasive for various reasons, including social stigma, lack of safe reporting channels and restrictive legal and cultural environments. These reporting barriers affect both men and women, and in many of the contexts where aid organisations work can be particularly challenging for individuals who identify as LGBTQI+.

---

104 Stoddard, A., Harvey, P., Czwarno, M. and Breckenridge, M. (2019) *Aid Worker Security Report 2019. Speakable: Addressing sexual violence and gender-based risk in humanitarian aid*. Humanitarian Outcomes (https://humanitarianoutcomes.org/AWSDR2019).

105 Cronin, E.A. and Afifi, A. (2018) *Review of whistle-blower policies and practices in United Nations system organizations*. Joint Inspection Unit, UN (https://digitallibrary.un.org/record/1643065?ln=en&v=pdf).

▶ *For more information on identity-based risks, see Chapter 1.2.*

Perpetrator profiles

Perpetrators may be external or internal to the organisation, for example staff, contractors and individuals belonging to armed forces, non-state armed groups and local communities. While perpetrators are more likely to be men, other genders can also be perpetrators or accomplices.

Perpetrators may be motivated by factors completely removed from their target's personal characteristics or conduct, such as personal circumstances, including family history, personality and behaviour (e.g. substance abuse), a permissive organisational environment and sexually aggressive peers. Perpetrators often rely on opportunities and allies to carry out their aggression, as well as environmental, cultural and societal factors, including power imbalances, cultural or societal justifications, perceptions of entitlement and a climate of impunity.

For more severe forms of sexual violence, perpetrators may attack their targets through coercion, incapacitation (e.g. using drugs or alcohol), or force (using weapons or physical strength). Perpetrators often require:

- means – the power, support and resources to offend;
- access – psychological or physical access to their target;
- knowledge – knowledge of their target's vulnerability or susceptibility;
- capacity – their ability to offend;
- motivation – willingness to offend; and
- opportunity – permissive circumstances or times to offend.

Organisational risk factors

Discomfort with discussing sexual violence and gender dynamics in organisations means that there are still insufficient conversations about this type of risk within aid organisations. The lack of direct and explicit attention to this issue can exacerbate the risk by contributing to permissive organisational cultures. Preventing serious incidents can depend on quickly responding to minor ones. Allowing minor instances of sexual violence or other forms of targeting, such as harassment, bullying and offensive jokes, can encourage more severe forms of violence, including sexual violence (this is sometimes described as a pyramid of violence[106]). Perpetrators take advantage of permissive environments and

106 For an example pyramid of violence, see EISF (2019).

may be influenced by aggressive peers. An organisation should ensure that no environment in which their staff work is a place where hostility of any kind – sexual or non-sexual – is the norm. Minor events need to be taken seriously, as these can be precursors to more serious incidents.

Organisational culture, including inclusivity, plays a strong role in determining whether incidents of sexual violence are reported and addressed. In the aid community, organisational cultures can often value toughness and macho attitudes (particularly in patriarchal contexts), which can further deter reporting. It is advisable for organisations to have clear guidance on what is a reportable offence as this can help staff understand when behaviour is not acceptable and feel empowered to take action.

All staff should be trained and feel able to address attitudes that can make sexual violence more permissive, such as discouraging offensive language. Managers and focal points play a particularly important role in ensuring their staff feel they can raise concerns. Through communication and outreach efforts, security staff can also shift organisational culture.

When the wider culture in an operational context is more permissive of sexual violence, it is especially important for organisational leaders to communicate and demonstrate through actions that what may be accepted outside of the office will not be tolerated by the organisational culture within it.

Climate surveys or targeted consultations

Staff-wide consultations can help organisations better understand organisational culture and whether attitudes and actions within the organisation are indicative of an environment that is permissive of sexual violence. These can take the form of 'climate surveys' – sometimes carried out by an external entity – which focus on perceptions of acceptable behaviour within the organisation. More targeted consultations ask specific questions around harassment, bullying and the concerns of particular groups of staff, for example female employees or individuals who identify as LGBTQI+.

External risk factors

Context analyses can help identify external factors affecting the risk of sexual violence, for example:

- High levels of sexual aggression in the broader environment.
- A failed or fragile state or other form of breakdown in law and order.
- Widespread impunity, including a criminal justice system that tolerates sexual violence or favours perpetrators.
- Active conflict or a militarised location.
- A conservative or patriarchal society.
- Power imbalances, for example between men and women or between ethnic groups.

These environmental risk factors enable sexual violence against local populations, and by extension those working for aid organisations. Sites of higher risk may include areas where armed groups operate, prisons and detention facilities, hotels and staff accommodation and border crossings and checkpoints. There may be times when risk is heightened, such as after dark, during busy events and when armed actors enter or leave a location. Attackers may sexually assault residents during compound raids. Sexual violence can also occur when aid workers are detained or held captive.

7.7.3 Risk mitigation: prevention and preparedness

Many sexual violence risk mitigation measures focus on regulating staff conduct. While an individual's vulnerability to sexual violence partly depends on the interaction between their intersectional identity (who the person is), behaviour, location, role and organisation (their intersectional vulnerability), sometimes there is nothing an individual can do to mitigate their inherent risk of being targeted. Like any other threat, measures must be taken at an individual and organisational level to reduce the risk.

The following is a basic overview of risk mitigation measures. For more detailed guidance, consult the GISF (formerly EISF) guide *Managing sexual violence against aid workers*.[107]

Governance

Policies, systems and mechanisms should be in place for preventing, preparing for and responding to incidents of sexual violence affecting staff. This can include

107 EISF (2019).

a policy of zero tolerance towards sexual violence and an organisational code of conduct that explicitly references all forms of sexual misconduct. These organisational instruments should be transparent and consistently applied, and include guidance on their practical implementation.

Good organisational practice includes developing clear policy statements about what support survivors can expect from the organisation following an incident. One international organisation found that ensuring that every incident of sexual assault and severe sexual harassment was reported up to the executive leadership team significantly helped with accountability.

Roles and responsibilities

How security staff are involved in managing sexual violence risks will vary by organisation. Security staff should ideally be equipped to: identify risk factors; implement respectful and inclusive risk mitigation measures; communicate threats appropriately; address inappropriate behaviour; recognise signs of a hostile environment; act as empowered bystanders (see the box below); and develop survivor-centred contingency plans that prioritise safety, confidentiality, respect and non-discrimination.

Empowered bystander

While a simple bystander might witness a situation without taking action, an empowered bystander, referred to as an 'upstander' within the UN, recognises harmful or unjust situations and takes steps to intervene, support those affected and prevent further harm. Empowered bystanders are equipped with the knowledge and confidence to act, whether through direct intervention, seeking help or providing support to those affected, while keeping themselves and others safe.

Within the UN, an 'upstander approach' to an event involves the following steps:

- noticing the event;
- interpreting the situation;
- taking responsibility;
- deciding to help; and
- intervening.

Human resources staff are often central in shaping policies and practices related to sexual violence, including developing and disseminating the code of conduct, creating duty of care policies for survivors and staff, guiding confidential response processes and leading internal investigations. They also carry out background checks designed to prevent the recruitment of sexual predators and establish disciplinary procedures.

A number of roles may be more directly involved in managing sexual violence risks and supporting survivors.

- **First responder.** The initial point of contact for a survivor of sexual violence, responsible for ensuring their immediate safety, providing emotional support, helping preserve evidence and facilitating medical care. This could be a trained staff member or a trusted colleague. Since all staff may be first responders, it is good practice to ensure they have access to guidance on psychological first aid.
- **Survivor supporter.** A survivor supporter acts as the primary point of contact between the survivor and the organisation. This individual should be equipped with training and guidance to offer emotional support, maintain confidentiality and assist the survivor in navigating the organisation's response protocols. It is good practice for organisations to allow survivors to choose their supporter.
- **Safeguarding focal point/ombudsperson.** Some organisations have established safeguarding focal points or ombudspersons to provide staff with a confidential means of reporting concerns. It is helpful to have both male and female focal points.
- **Internal investigators.** The individuals conducting an internal investigation into allegations of sexual violence must be entirely independent of the survivor, the alleged perpetrator and their respective management lines.

Induction, briefings and training

All staff, no matter their location, are at risk of sexual violence as this risk exists in every country and can even be perpetrated online. Organisations should ensure that all staff, no matter their role or location, are informed of the nature and forms of sexual violence they may encounter in their work. They should be made aware of online threats, the risk of date rape drugs and that perpetrators may be known to them and may even be a colleague. Staff can also be made aware of contextual and other factors that may place certain profiles at higher risk than others. This enables staff to:

- understand what the organisation has in place to reduce risk;
- understand what procedures and rules they need to follow;
- use this information to identify their own personal risk profile (which may be unique due to their intersectional identity); and
- get advice from focal points and work with their organisation to reduce risk.

▶ *See Chapter 1.2 on identity-based risks.*

Staff inductions and orientation briefings cover policies, reporting and accountability mechanisms in relation to sexual violence. To respect cultural norms, the organisation may choose to deliver briefings and training to male- or female-only groups. By considering local attitudes, the organisation can tailor its approach to encourage open discussions on sensitive issues.

Security training can provide important information on sexual violence risks, such as how staff can reduce their risk and respond in the event of an incident. This can include guidance around culturally appropriate conduct, when and how to report incidents or concerns, how to travel (e.g. in larger groups), how to set personal boundaries and which areas, times and groups to avoid. All staff benefit from training on local risks and prevention strategies, their specific roles and responsibilities in responding to sexual violence, and the importance of protecting confidentiality when incidents are reported. It may be advisable to provide guidance on collecting and preserving evidence should the survivor choose to pursue a case.

Inductions and training are an opportunity to foster a positive organisational culture, with the organisation sending the message that violence in any form is not acceptable and no one is ever to be blamed if they are a target of sexual violence.

Some organisations train their staff on bystander intervention, which can be an effective strategy for preventing sexual violence. Training can include interactive elements such as role-playing and discussions tailored to the specific context.[108]

Inclusive risk assessments and security plans

An inclusive risk assessment should identify high-risk places, times and situations, as well as considering how factors such as age, sex, nationality, race, sexual orientation, disability, appearance and behaviour affect individual vulnerability.

108 For more guidance, see EISF (2019), Tool 2, bystander intervention (pp. 94–95).

A comprehensive risk assessment should integrate individual, organisational and external risk factors. This assessment should address both external and internal threats, recognising that perpetrators may be employees, and understand potential perpetrator profiles.

The risk analysis can draw from various sources, including internal reporting systems, confidential consultations with staff and the local community, and insights from focal points in other aid or human rights organisations. Discretion and sensitivity to cultural and social norms may be necessary when gathering information.

Guidelines and SOPs for responding to sexual violence must be clear and readily available to staff. They should carefully avoid a framing that suggests 'advance victim-blaming' and give equal attention to understanding and deterring would-be perpetrators.

Organisational contingency plans (such as evacuation or relocation of affected staff) must also consider sexual violence risks and what support is available in the short and longer term. It can be beneficial to discuss with staff from various cultural backgrounds what prevention measures, protocols and support they find most appropriate. These consultations ensure that the organisation responds effectively in each context and does not cause further harm.

Identity-based mitigation strategies

In some circumstances, security procedures may differ for certain groups of staff if the risk assessment indicates that their personal profile places them at higher risk of sexual violence. The following key questions can be considered to avoid undue discrimination.

- Does the risk assessment consider personal characteristics and robustly indicate the differentiated risk across staff profiles (this involves considering all identity characteristics and their intersectionality, including sex, sexual orientation, ethnicity and visible and invisible disabilities)?
- Have affected individuals been informed of their heightened risk (acknowledging they may already be aware of this) and had the opportunity to discuss risk mitigation measures?

- Could less extreme forms of risk mitigation be implemented? A blanket ban or removal of a group of staff is a common risk mitigation strategy, but other measures may be more acceptable and appropriate to the circumstances. Consultations with affected staff can help identify alternative security risk management options.

▶ *See Chapter 1.2 – Person-centred approach to security for a more detailed discussion on differentiated risks.*

Incorporating sexual violence risks into security procedures

Security procedures should consider any heightened risk of sexual violence.

- **Site security.** Hotels and accommodation used by staff should offer maximum protection from intruders. In some cases, the risk assessment may indicate that staff at particularly high risk, such as female staff, could be lodged with colleagues or in specific areas judged more secure.
- **Travel security.** Staff need to be briefed on appropriate travel procedures and how to protect themselves and others against the risk of sexual violence while on the move. Staff considered at high risk (international or national) can be accompanied from home to work in an organisation vehicle. At-risk staff can travel either in groups or accompanied by others – inside and outside work hours. In a particularly high-risk environment, it may be advisable for at-risk staff members not to be left on their own, even for short periods.
- **Information security.** Staff members' personal details should not be displayed outside their residences or listed in the telephone directory. Security measures should be in place to protect staff from unwanted disclosures relating to their identity and whereabouts, both online and offline.

- *To learn more about site security measures see Chapter 7.2.*
- *For more guidance on travel security, see Chapter 7.1.*
- *For more on information and communications security, see Chapter 6.1.*

Contingency planning

Service providers

Creating a network of competent service providers, including medical and psychological professionals, in all operational contexts can ensure timely support for survivors of sexual violence (which should ideally be given within 24 hours after an incident takes place). This network should be thoroughly evaluated for responsiveness and capability. Attitudes towards survivors can also be assessed to ensure that they do not cause further harm through victim blaming or inappropriate remarks.

All staff should have access to emergency medical treatment, including emergency contraception, HIV post-exposure prophylaxis (PEP) kits and other medicines to reduce the risk of disease transmission. In remote areas, PEP kits may be stored by the UN, ICRC and/or medical NGOs. If PEP kits and other specialised medication are not readily available from medical institutions or other agencies in the area, organisations can ensure that they are on hand in the office and can be dispensed under medical supervision (as side-effects need to be monitored), or that the survivor can be transported immediately to somewhere where they are available. Organisations should pre-identify safe locations for medical examinations and care, and set up referral procedures. Known and trusted private clinics can be used if the survivor chooses not to report the incident.

Organisations with particular restrictions (for instance, against contraception) should inform staff of this more generally.

- *See Chapter 5.4 for more on staff care.*
- *See Chapter 5.5 for more medical and health considerations.*

Logistics

Logistical arrangements include reliable transport for the survivor and an accompanying individual, as well as provisions for confidential relocation or repatriation of survivors, if necessary.

Insurance

With the survivor's consent and where insurance policies are in place, it is crucial to inform insurance providers promptly about the incident to ensure that the survivor can access medical and psychological support. The timing of this notification can vary depending on existing agreements with the insurance provider(s) and organisations should be aware of the minimum information required by insurers to initiate support. Protocols should be established for maintaining confidentiality.

It is also helpful to have clear agreements with insurance providers regarding the specific types of coverage available for incidents of sexual violence. This includes understanding the scope of medical care, psychological counselling and other psychosocial support, and any potential legal support. Ensuring that these areas are explicitly covered in the policy can prevent delays and complications when an incident occurs.

▶ *See Chapter 5.4 for more on insurance.*

Legal considerations

Organisations should be prepared to advise survivors on their options, including the implications of reporting to local authorities and the legal definitions of sexual violence in that context. Relationships should be established with trusted local legal professionals who can provide immediate assistance if needed. For more legal considerations, see section 7.7.4 below.[109]

Reporting and whistleblowing

Robust and confidential reporting and whistleblowing mechanisms not only support incident response, but can also deter potential perpetrators. Responsible staff should ensure that these mechanisms are confidential and accessible to all staff regardless of position and language. Staff should be encouraged to report even minor incidents. Sexual violence reporting channels may be separate from reporting mechanisms for other security incidents due to the need for additional confidentiality. Unofficial reporting of sexual violence

109 For more detailed guidance, see EISF (2019), Tool 3, legal environment questionnaire (pp. 96–98).

incidents (for example via medical services, counselling and surveys) may be considerably higher than incidents reported through official channels.

It is good practice for organisations to offer staff several confidential reporting channels, including options to raise concerns anonymously, formally and informally. Staff in an office may not speak up if all reports go to one senior manager, who may be the perpetrator or an ally of the perpetrator. To address this risk, one international NGO has introduced a third-party ethics and compliance service provider to host an online whistleblower website to report ethical concerns or misconduct involving the organisation's staff.

Designated safeguarding focal points/ombudspersons can help staff who require more information, are unsure whether an incident is severe enough to merit a formal complaint, or are afraid of the repercussions of reporting.

Finally, organisations should be transparent about what happens following a report, including what investigations and disciplinary actions may take place and how the reporter may be involved in the process. Reporters should be provided with regular feedback on how their report is being actioned. Need-to-know information-sharing protocols can be followed, limiting information to a minimum number of individuals. Maintaining a secure log of all communications and decisions regarding the response may also be advisable.

Case example: Failures in whistleblower protection

In 2009, a volunteer aid worker was murdered in Benin after she reported to her country director concerns that a contractor for the agency was sexually abusing local community members. Investigations into the incident indicate that failures in confidentiality may have allowed the whistleblower's identity to be revealed to the alleged perpetrator, who had personal connections within the organisation. The case highlights many shortcomings, including a lack of safe and confidential reporting mechanisms, robust investigation processes and security measures to protect whistleblowers.

Source: Peace Corps Office of Inspector General (n.d.). *Resources: Kate Puzey Volunteer Protection Act of 2011* (www.peacecorpsoig.gov/resources/resources-kate-puzey-volunteer-protection-act-2011).

When logging incident reports within the organisation's incident information management system, security staff will want to consider how to ensure confidentiality when names and other details may be required fields. Some organisations keep these types of incident reports separate for confidentiality reasons. Reporting is necessary for security risk management and risk analysis, but this needs to be balanced with the safety, psychological wellbeing and privacy rights of the survivor.

Recruitment, investigations and disciplinary action

Rigorous screening for potential employees, including thorough background checks and reference checks across multiple countries, can prevent known sexual violence perpetrators from moving between aid organisations. Several safeguarding initiatives in recent years have focused on supporting organisations with this.[110]

Organisations should have a formal process for investigating reports of sexual violence, with adapted measures if the alleged perpetrator is employed by the organisation. Allegations against staff members should be followed by an internal investigation and disciplinary action if applicable. If the survivor wishes to pursue justice, the authorities may be brought in. Offenders, allies and enablers should be held accountable by the organisation. To deter further offences, non-compliance with policy and investigations should result in disciplinary action.

7.7.4 Response

Timely responses to sexual violence incidents are critical to ensure the safety and wellbeing of those affected. How an organisation responds will depend on various circumstances, including when the incident took place, the wishes of the survivor, the severity of the incident and the risks posed to others. Some overarching things to keep in mind when responding are as follows:

- Survivors of sexual violence can report incidents immediately, days, weeks, months or years after the incident. Factors that influence when an incident is reported include safety, culture and the psychological and emotional impact of the event on the survivor. Organisations should treat all reports as a priority, no matter when the incident took place.
- Organisations should be prepared to inform survivors of any relevant cultural and legal considerations. In some regions reporting sexual violence could lead to additional harm for the survivor due to local laws and cultural practices.

110 For example, the Misconduct Disclosure Scheme: https://misconduct-disclosure-scheme.org/

- The risks of re-traumatisation, self-harm and suicide are very high. It is imperative that responders are trained to provide adequate support and maintain confidentiality.

Good practice highlights the need to ensure that responses to sexual violence incidents are guided by survivor-centred care, which respects the survivor's wishes as much as possible, as long as these wishes do not put them, colleagues or the organisation at risk of harm. A survivor-centred approach is responsive to a survivor's needs and preferences, and seeks to protect survivors from stigma, discrimination, retaliation or other harmful consequences. The approach aims to create a supportive environment in which the survivor's rights, safety and confidentiality are respected and prioritised, and in which the survivor is treated with dignity and respect. The approach aims to support the survivor's recovery by enabling them to choose the support and care they need; lead decisions about optional reporting; and decide if/how they wish to be involved in any investigation. This is distinct from a survivor-led approach, which leaves all decision-making power with the survivor, even if these decisions may place them or others at risk of harm.

▶ *For more details on the survivor-centred approach, see Chapter 5.4 on staff care.*

Communicating with the survivor

As with all traumatic events, how individuals and the organisation interact with a survivor plays an important role in healing and recovery. Psychological and emotional support can come from colleagues and friends, through peer support networks and compassionate interactions. Any communication with the survivor should aim to:

- make them feel safe;
- make them feel in control;
- make them feel believed and heard; and
- make them feel that the organisation is taking the incident seriously.

Communication should not:

- imply the survivor is to blame or judge them in any way;
- minimise their experience;
- force companionship or other support on them;
- tell them how they should be acting or feeling, or normalise their response; or
- place pressure on them to make decisions or act.

Initial response

When an individual experiences sexual violence, particularly a severe incident, timing is key. Often, it helps to prioritise actions into a response timeline identifying immediate, short-term and long-term needs. It is also important to recognise that everyone's experience is different. Some may require immediate medical and psychosocial support, whereas others may request support later. There is no 'correct' path. However, as it relates to some aspects of response, such as medical care and reporting, timing may play a larger role.[111]

Depending on the severity, the organisation's incident management structure may need to be activated, including providing family and communication support functions. The first responder, responsible focal points or the incident management team (for severe incidents) will usually oversee some or all of the initial response activities outlined below. Due to their sensitive nature, many organisations may set up a separate incident response team to handle sexual violence cases.

► *See Chapter 4.4 for more details on how to manage critical incidents.*

- **Safety and security.** Ensuring the survivor's immediate safety and that of others at risk is the top priority, while maintaining confidentiality to protect the survivor.
- **Medical care.** Emergency medical care, including treatment for injuries, infections and prevention of pregnancy, should be provided with the survivor's consent as quickly as possible. Survivors of sexual assault may

111 EISF (2019) presents a detailed response framework of key steps responsible staff can take at different times.

require emergency contraception, prophylactic treatment for sexually transmitted infections, PEP for HIV and medicines for other diseases such as hepatitis B. All of these should be initiated as soon as possible after the incident.

- **Psychosocial care.** Immediate access to appropriate psychosocial support should be offered.
- **Identifying a survivor supporter.** Organisations can ask a survivor who they would like to be their supporter, or offer access to an organisation-trained survivor supporter.
- **Family liaison.** With the survivor's consent, their family can be informed through a designated contact person, following strict confidentiality guidelines.
- **Location.** Survivors may need to be housed in a secure, confidential location close to supportive individuals, with relocation or evacuation if necessary.
- **Incident reporting.** The incident should be reported through appropriate channels, while safeguarding the survivor's safety and privacy.
- **Support and guidance.** The organisation should be clear that they believe the survivor's account and provide clear guidance on next steps, ensuring ongoing communication and support throughout the process.[112]

In the longer term, additional administrative and logistical support may be needed, such as arranging financial assistance for the survivor and support staff, organising private transportation for those involved in the response process, suspending work duties for affected staff, agreeing on how to communicate about the survivor's absence to colleagues, and establishing regular check-ins to address ongoing needs and concerns with survivors. Insurance providers may also need to be informed, with the survivor's consent.

Support may need to be offered to other staff members, such as witnesses and the wider team. Supporting sexual violence survivors is stressful and demanding. Those doing so can be offered emotional and psychosocial support, including taking breaks or stepping away.

112 For more detailed advice for first responders, see EISF (2019) *Tool 5, guidelines for a survivor supporter* (pp. 58–61).

Online risks of sexual violence

Online forms of sexual violence are an increasing concern for aid organisations. While anyone can be a target, women and LGBTQI+ individuals are disproportionately affected, necessitating tailored prevention and response measures. Risks include harassment, stalking and cyberstalking, sexual extortion and the non-consensual sharing of intimate images.

▶ *See Chapter 6.2 for more details on digital risks and mitigation measures.*

Response considerations

Focal points or the incident management team may need to address some of the more complex response considerations discussed in the following section.

Confidentiality and communications

Organisations must proactively manage communications in the event of a serious sexual violence incident by establishing clear internal and external protocols, considering the implications of sharing information about the incident and the perpetrator, and ensuring the confidentiality and safety of the survivor. At the same time, organisations should respect the survivor's right to speak out, if they wish, and should provide guidance and support, including access to trained focal points who can help navigate the potential risks and consequences of public disclosure.

If the incident is publicly known, media management may be required.

▶ *See Chapter 4.4 for more details on media management.*

Reporting to the police and legal proceedings

Organisations should ensure that they have a comprehensive understanding of the legal environments in which they operate, particularly concerning incidents of sexual violence, with access to local lawyers to provide guidance and support in the event of an incident.[113]

The organisation can assist the survivor with any legal and justice processes they choose to pursue. This includes accompanying them to report the incident

113 For more detailed guidance, see EISF (2019) *Tool 3, legal environment questionnaire* (pp. 96–98).

to the police, supporting them if a police interview is required, and ensuring their safety and wellbeing during any evidence-gathering processes. Collecting evidence does not commit the survivor to legal action but preserves the option for the future. Reporting an incident to the police can itself be a traumatic experience, even in the best of circumstances.

Organisations may also need to secure appropriate legal representation for the survivor. The organisation's legal adviser can help clarify procedures and timelines for reporting, as obtaining official documentation can be crucial if the survivor later decides to press charges or seek further treatment. The decision to prosecute rests with the survivor and they should feel supported and empowered to make an informed choice.

More broadly, organisations must understand the legal requirements for reporting sexual violence incidents to the police in the country, including any obligations to report, implications for the survivor and alleged perpetrator, and whether they must remain in the country after reporting. Some foreign nationals might choose not to report incidents to the police if this would require them to remain in the country until the trial concludes (which could take several years). In some countries, survivors may face charges of adultery or fornication if they cannot prove assault. This can result in punishment for the survivor rather than the perpetrator. Organisations must also consider the impact of legal action on alleged perpetrators, especially if they are staff.

If legal proceedings are pursued, prosecution will usually occur in the country where the incident took place and may require the collection of medical evidence. The risk of further trauma is immense in these circumstances, and it is advisable for the organisation to be prepared to help survivors navigate these procedures safely e.g. pre-identifying trusted medical facilities and local forensic evidence collection expectations. Some medical facilities that treat survivors may also automatically file reports with the police.

In some cases the focus may be less on whether the incident took place and more on whether it was consensual, which can throw up different challenges.

Case example: A second traumatic experience

It is not uncommon for a survivor to suffer a second trauma as a result of insensitive treatment by the police. In one case a female international aid worker was sexually assaulted while working outside of her home country. No one in the organisation knew what to do immediately after the incident. The next day she was sent, alone, to her embassy to report the incident.

The embassy sent her to the local police accompanied by the embassy security officer, a national. Once at the police station, four armed policemen interrogated her, asking detailed questions about the incident. When she hesitated in her answers, they accused her of lying. During the interrogation other policemen kept coming in for a look, as they were curious. The police undertaking the interrogation insisted that she show them her injuries before she was allowed to leave the station. They then insisted on her taking them to the place where the incident took place, for a re-enactment which they claimed was essential to the investigation. No real investigation ever took place. The assailant was never caught, and the survivor learned later that it was very rare for anyone in that country to be tried or convicted of sexual assault. Her experience at the police station was effectively a second assault.

A well-informed and trusted individual should always accompany the survivor to the police station, to ensure that they are not intimidated or further victimised, that interviews are conducted in a language the survivor understands, and that appropriate documentation and assistance are provided. The accompanying individual may need to be prepared to intervene if the survivor's rights and dignity are not respected. It is important that this individual takes on the role as an organisational representative and is not perceived as acting in their individual capacity.

When the alleged perpetrator is a member of staff

When an alleged perpetrator of a sexual violence incident is a member of staff, organisations may need to take a series of immediate and carefully considered

actions, including safeguarding both the survivor and others who may be at risk of further harm, as well as protecting the alleged perpetrator. Alleged perpetrators can pose continued security risks to the survivor and other staff, including staff investigating allegations.

If the allegations are serious, the organisation may decide to suspend the alleged perpetrator or place them on administrative leave (while maintaining confidentiality about the reason for their absence). If the alleged perpetrator poses a risk or is in danger themselves due to the allegations, they may need to be relocated to a secure location and accompanied during their stay. It is usually advisable to prevent any contact between the survivor and the alleged perpetrator, particularly in severe cases, although the survivor's preferences regarding contact should be considered.

It is important that trained and independent investigators conduct the process (supported by relevant departments such as HR and security) to prevent re-traumatisation or further harm.[114] A poor investigation can be profoundly harmful to the survivor, the alleged perpetrator and others impacted by the incident. Failing to address an allegation can have equally damaging consequences.

7.7.5 Post-incident actions

Aftercare

Affected staff may require long-term aftercare following a sexual violence incident. Organisations should put in place a supportive framework while avoiding overwhelming survivors with decision-making. It is imperative that an organisation's policy clearly outlines the extent, cost and duration of the support it can realistically offer survivors, ensuring they are not misled about the availability of indefinite assistance.

Survivors may require ongoing medical support, including regular health checks and treatment for any physical health issues. Survivors may need long-term psychosocial support to cope with trauma, anxiety, depression and other mental health issues that can arise after an incident. This support should be tailored to the individual's needs, and provided by trained professionals experienced in handling trauma.

114 For a detailed internal investigation process, including key steps, see EISF (2019).

A comprehensive long-term survivor support plan can be developed, taking into account the survivor's preferences and needs. This may include medical and psychological assessments and therapies, logistical support for aftercare, an evaluation of work options, a work reintegration plan and a transition to long-term support services (such as national services), along with a communication and check-in schedule. The length of any legal proceedings should be factored into the support plan. The support plan should be flexible to adapt to the evolving needs of the survivor over time. Trauma can manifest many months or even years after an incident, and it may be difficult to anticipate when or how triggers will arise. Ideally, survivors should have easy and straightforward access to psychosocial resources and care, even if they need support months after the incident or after their employment has ended. It is important to remember that cultural factors can significantly influence an individual's response. When providing support, organisations should remain open and sensitive to the various paths to recovery and the survivor's preferences.

▶ *See Chapter 5.4 for more on staff care.*

Post-incident review

Finally, organisations should conduct thorough post-incident reviews, while maintaining strict confidentiality to protect the staff involved, to assess the handling of severe incidents of sexual violence and identify areas for improvement.

▶ *See Chapter 4.4 on incident response and crisis management for more guidance on post-incident reviews.*

Further information

Guidance

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

EISF (2019) *Managing sexual violence against aid workers: prevention, preparedness, response and aftercare* (https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/).

EISF and InterAction (2014) *NGO Safety and Security Training Project: how to create effective security training for NGOs* (https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos).

GISF (2022) *Managing sexual violence against aid workers* [*Training*]. DisasterReady (https://ready.csod.com/ui/lms-learning-details/app/course/581feec5-4ce2-493a-9266-90ed6099bc48).

IASC (2023) *IASC definition & principles of a victim/survivor centered approach* (https://interagencystandingcommittee.org/iasc-champion-protection-sexual-exploitation-and-abuse-and-sexual-harassment/iasc-definition-principles-victimsurvivor-centered-approach).

IASC (n.d.) *Protection from sexual exploitation and abuse* (https://psea.interagencystandingcommittee.org/).

Karaman, S. (n.d.) *Online harassment of politically-active women: an overview.* XYZ, Tactical Technology Collective Project (https://xyz.informationactivism.org/en/online-harassment-of-politically-active-women-overview/).

PEN America (n.d.) *Best practices for employers. Online harassment field manual.* (https://onlineharassmentfieldmanual.pen.org/best-practices-for-employers/).

Persaud, C. (2012) *Gender and security: guidelines for mainstreaming gender in security risk management.* EISF (https://gisf.ngo/resource/gender-and-security/).

Safeguarding Resource & Support Hub (n.d.) *Together, we can build a safer sector* (https://safeguardingsupporthub.org/).

Steering Committee for Humanitarian Response (n.d.) 'Misconduct disclosure scheme' (https://misconduct-disclosure-scheme.org/).

Research and discussion

Cronin, E.A. and Afifi, A. (2018) *Review of whistle-blower policies and practices in United Nations system organizations.* Joint Inspection Unit, UN (https://digitallibrary.un.org/record/1643065?ln=en&v=pdf).

Deloitte (2019) *Safe space survey report* (https://viraltopiczone.wordpress.com/wp-content/uploads/2019/01/d3bcc-un_safe_space_survey_report_15_january_2019_final.pdf).

Humanitarian Women's Network (HWN) (2016) *Full survey results* (https://interagencystandingcommittee.org/sites/default/files/migrated/2016-11/hwn_full_survey_results_may_2016.pdf).

Mazurana, D. and Donnelly, P. (2017) *STOP the sexual assault against humanitarian and development aid workers.* Feinstein International Center, Tufts University (https://fic.tufts.edu/publication-item/stop-sexual-assault-against-aid-workers/).

Nobert, M. (2017) *Humanitarian experiences with sexual violence: compilation of two years of Report the Abuse data collection*. Report the Abuse (https://reliefweb.int/report/world/humanitarian-experiences-sexual-violence-compilation-two-years-report-abuse-data).

Peace Corps Office of Inspector General (n.d.) *Resources: Kate Puzey Volunteer Protection Act of 2011* (www.peacecorpsoig.gov/resources/resources-kate-puzey-volunteer-protection-act-2011).

Stoddard, A., Harvey, P., Czwarno, M. and Breckenridge, M. (2019) *Aid Worker Security Report 2019. Speakable: addressing sexual violence and gender-based risk in humanitarian aid*. Humanitarian Outcomes (https://humanitarianoutcomes.org/AWSDR2019).

7.8 Detention and arrest

The effective management of incidents of detention and arrest requires planning and investment in local capacities and well-established response protocols. Detention and arrest situations will usually require implementation of an incident response plan (described in Chapter 4.4.). In any of the scenarios discussed here, the priority is the safe and speedy release of the staff member. To achieve this, the organisation needs an informed response approach, which is likely to include mobilising support from local stakeholders.

7.8.1 Definitions

It is important to differentiate between detention and arrest, both for reporting and for effective response.

Detention refers to the holding of a person against their will by an individual or group (e.g. community groups, local authorities, militia or military groups). While there is no intention to harm the detainee, there is also no clear condition for their release. Detention can be a frequent occurrence in aid work; both short and long detentions are common. Purported grounds for detention may include incorrect credentials or administrative documents, while underlying causes can range from discontent with programme quality or location, mistaken identity of the aid worker or organisation, suspicions and misinformation, to simple bribe-seeking. There may also be frustration that the authorities are not engaging with a particular group, or are not doing so in a satisfactory manner; aid workers can often be seen as a source of leverage.

Arrest refers to formal detention by an official authority (normally the police but also the military) or the presumptive authorities. Arrest differs from the more general type of detention mentioned above in the involvement of official authorities invoking their legal powers. The situation can be more difficult and dangerous when government authorities arrest someone extralegally (i.e. without a proper arrest warrant), or where the arrested person 'disappears'. The authorities may then deny that the arrest took place and may refuse to reveal the whereabouts of the arrestee.

7.8.2 Risks

The risk of detention and arrest increases in contexts where there is a substantial reliance on humanitarian aid, where there is negative sentiment towards an aid organisation or aid work in general and where there are political or financial incentives at play. These types of incidents carry secondary risks that must also be considered:

- Risks to the health, safety and wellbeing of detained/arrested staff, especially if they experience violence, have medical conditions or have experienced trauma in the past. Being held against their will may exacerbate existing mental health issues. They may also lack access to medical care, basic freedoms, privacy, interpreters, legal counsel or other support.
- Operational disruption, especially if key staff are held for prolonged periods. A common strategy is to withdraw and suspend programming while the release is arranged.
- Risks to the organisation's reputation and relationships with local communities, donors and partners. This could jeopardise the organisation's ability to operate.
- Risks of staff being held in inappropriate facilities, especially if they have particular vulnerabilities.
- Risks to colleagues tasked with supporting or visiting detained/arrested staff. These individuals risk intimidation and retaliation, as well as the stress of the role.

Aid organisations can plan and prepare for these types of incidents, especially in contexts where the risk is high, and have well-established response mechanisms in place.

7.8.3 Planning, preparedness and risk mitigation

Effective planning and preparedness are crucial for mitigating the risks associated with the arrest and detention of aid workers. Note that preventing an arrest that follows legal procedure is obviously not normally possible. While an arrest that does not follow proper legal procedure can be challenged, it is unlikely to be preventable.

As part of their planning and preparedness, organisations should ideally design multilayered and detailed contingency plans to protect their staff and ensure the continuity of their operations with respect to both detention and arrest risks.

Context, risk analysis and contingency planning

- **Detention and arrest risks are incorporated into security risk management.** Risk assessments and contingency planning include the risk of detention and arrest. Contingency plans include evacuation and extraction procedures. Context analyses include an overview of the political, security and legal environments in areas of operation.
- **Actor mapping** can support access and negotiation and efforts to develop relationships with local communities, authorities and other stakeholders, which can help facilitate a rapid response to an arrest or detention.

Legal preparedness

- **Understanding of the legal and political context of the operating environment.** Staff need to be made aware of the hierarchy of the national security forces or other de facto authorities in the organisation's area of operation. This can include clan and community structures, and being clear about the legal procedures governing arrest in the country.
- **Legal briefing.** Staff should be informed about local laws, their rights and procedures to follow if detained or arrested. Organisations should be clear on what kind of support may be provided to detained and arrested staff, including support after release and to family members.
- **Legal support.** It is advisable to establish connections with local legal professionals and international legal aid organisations who can provide immediate assistance.
- **Regular monitoring.** Responsible staff can review and report on detention and arrest trends in the operational context, and the actors involved.

Training and awareness

- **Keeping updated local response plans.** Clear protocols should be maintained and staff should know the procedures for reporting and responding to detention and arrest incidents, which stakeholders to notify, and roles and responsibilities within the organisation. Plans should include communication protocols and escalation procedures, as well as measures to ensure continuity of operations if key personnel are detained or arrested.
- **Security training**. Orientation and training should be provided to staff on personal security measures, situational awareness, risk avoidance and protocols during interactions with authorities.

- **Scenario drills.** Regular drills and simulations allow staff to practise response procedures in case of detention.
- **Documentation.** Staff should be made aware of the documentation they need to carry and other measures they need to follow in order to gain access to and travel safely in operational areas.

Advocacy and networking

- **Communication roles and responsibilities.** Aid workers should be able to explain their roles and the organisational mission in simple and engaging terms. This may need regular practice.
- **Stakeholder engagement.** Staff should engage with local authorities, community leaders and other stakeholders to build relationships and reduce the likelihood of an incident.
- **International advocacy.** Organisations can work with each other and through diplomatic channels to advocate for the protection of aid workers.

Staff care

- **Staff care protocols** (including mental health support and counselling) can be established covering staff before, during and after an incident.

► *See Chapter 5.4 on staff care.*

Family liaison

- **Working with families** is critical in effectively responding to medium- to long-term situations. Relatives may be responsible for feeding and maintaining the health of their detained/arrested family member. They are also likely to have to manage bail and payments of fines. Consider establishing protocols for support of and communication with the families of detained/arrested staff, including what financial or legal support can be provided, and under what conditions.

Monitoring and evaluation

- **Regular reviews and reporting.** Organisations can conduct regular reviews and updates of risk assessments, contingency plans and training programmes. This helps to identify progress and acts as an early warning for future risks.
- **Incident analysis.** Interviews and reviews of arrest or detention incidents can help identify lessons and improve future responses.

Some staff may be detained or arrested for reasons extraneous to their work or that of the aid organisation. Factors that may play a role include social or cultural affiliations, power dynamics and political or criminal activity. Aid organisations should have a clear policy about how much support they will provide in the case of non-work-related arrests or detentions. If the detention or arrest is due to political circumstances, aid organisations may be wary of being seen as meddling in local politics. This should not, however, be an automatic barrier to assuming responsibility for staff in this situation, and making every effort to ensure their safe return.

7.8.4 Responding to an incident

When staff members go missing, the first challenge is to find out and report the exact nature of the situation. This might take hours, days or even weeks. Basic information needs to be established and communicated in an incident report that is then shared with appropriate staff.

Good practice involves being clear on who has been or should be notified, and who already knows about the incident outside the organisation, including whether the police, security forces or authorities are aware, have been or will be informed; whether the press or any third parties are aware of the incident; and whether next of kin have been notified. Information management can be challenging but should be carefully considered and addressed by staff leading on the response. Monitoring of the press, social and other media should also be considered; this can include local, national, regional and international media.

Organisations need to consider privacy and confidentiality around reporting or sharing information. During longer-duration situations, an organisation may decide to elevate their response and start a public advocacy campaign to secure the release of a staff member or highlight their condition. This should ideally be done with the staff member's permission.

Incident response procedures are discussed in more detail in Chapter 4.4. Below are some more detailed considerations.

In the event of detention or arrest

In the event of a detention, a heavy-handed approach is likely to be counterproductive, and can increase antagonism towards the staff member and the organisation. The detention may be designed to force the organisation or another entity to pay attention and engage in serious dialogue, in which case responding to this expectation can be enough to end the incident.

In some cases the detainee may be able to negotiate their own release, and organisations should train staff accordingly. Emphasising their humanitarian work and the neutral, impartial and independent nature of their organisation and its activities is often an important first step, and some organisation staff carry with them aide-memoires or other documentation to clarify the role of the organisation. Carrying emergency contact information is also helpful in the event of a detention.

If a staff member is arrested and their whereabouts are unknown, the first priority is to establish where they are and under whose authority. This may entail visiting relevant local authorities, informing the embassy (in the case of a foreign national), and using local networks to gather details. It is important to remember that a staff member may be arrested for legitimate reasons and may have to account for their actions. Either way, organisations may consider engaging a good local lawyer who knows the local languages and the local system, has experience with this type of situation, and has useful connections.

When it is clear who has detained or arrested the staff member and where they are, organisations should seek to ensure that their rights are protected. Organisations should consider advocating with local authorities for the fair and humane treatment of affected staff, including access to medical care, legal counsel and due process. This can be done after an assessment and conversations with stakeholders, as the attention of an international organisation may exacerbate the situation. Additional actions may be considered if these requests are not met. Any mistreatment or rights violations should be documented, and accountability pursued if appropriate (being mindful that this can cause more harm than good).

Arrests can be made without formal charges being brought, in which case the organisation might advocate for a charge to be articulated within a specified period of time. The charge may relate to the individual (for example, they are accused of being involved in a crime) or the organisation (for example, an accusation of spying under cover of humanitarian work). In any scenario, the

main priority is to work towards the safe and speedy release of the staff member. In most circumstances, only once a staff member is freed from wrongful charges should efforts be made to clear the name of the individual or the organisation.

As part of a broader contingency plan, the organisation may need to discuss what administrative and financial support will be provided to the affected staff member and their family. Under what circumstances would legal support be arranged or bail paid? By what means and who would be responsible? Many organisations will have insurance covering some of these contingencies. Consideration may need to be given to whether the cover is applicable and extends to all staff or just key individuals. This may be considered at the policy level as part of a broader risk management position.

▶ *See Chapter 5.4 for more on insurance.*

Organisations may want to provide additional support to individuals whose role it is to visit detained/arrested staff and liaise with authorities, as this can be a challenging task with many potential repercussions on the staff member (e.g. their mental health, as well as their relationships with local authorities or groups). This role should not randomly fall to an individual based on their proximity to the context. It is also critical to liaise with, and manage, the staff member's family in the event of an arrest or a detention. They should ideally be informed of the steps being taken; organisations should aim to maintain a direct regular line of communication, remain aware of what steps the family intends to take or has taken, and warn them if what they plan to do has the potential to disrupt, complicate or be counterproductive to the organisation's planned response.

▶ *See Chapter 4.4 for more on family liaison.*

It is likely that support from the local community and stakeholders will be influential in securing the release of a detained/arrested staff member. Clan and social dynamics might be mapped and interlocutors identified to support enquiries and requests. Organisations that are not local to the area may find information from local actors useful in maintaining a check on the condition of affected staff and passing on informal messages.

Post-incident considerations

Released staff members and those closely involved in the incident, such as family members or the incident management team, may require additional support following an incident. This can include a break from work, medical support and counselling.

► *See Chapter 5.4 for more on post-incident staff care.*

It may be helpful to talk to relevant authorities, stakeholders and community leaders as to why the detention or arrest took place, and what can be done to avoid a similar incident in the future.

Many organisations will hold a formal factual debrief session or after-action review.

► *See Chapter 4.4 for more on after action reviews.*

Further information

Guidance and resources

Buth, P. (2010) *Crisis management of critical incidents.* EISF (www.gisf.ngo/resource/crisis-management-of-critical-incidents).

Davidson, S. (2013a) *Family first: liaison and support during a crisis.* EISF (www.gisf.ngo/resource/family-first/).

Davidson, S. (2013b) *Managing the message: communication and media management in a security crisis*. EISF (www.gisf.ngo/resource/managing-the-message).

Hostage International (n.d.) *Best practice in family support* (https://hostageinternational.org/resource/best-practice-in-family-support/).

Hostage US (n.d.) *Hostage US guides* (https://hostageus.org/resources/hostage-us-guides).

7.9 Abduction, kidnapping and hostage situations

Incidents of abduction – including kidnapping and hostage situations – can entail long-lasting physical and emotional impacts. Preventing, preparing for and responding to an abduction requires organisational investment and planning. This chapter covers good practice in managing abduction risks. It includes guidance on virtual and express kidnappings, which have become more prevalent in recent years, and addresses the long-term impacts and other enduring issues associated with abductions.

7.9.1 Definitions

Abduction refers to any illegal, forcible capture of a person. Kidnapping refers to an abduction with the explicit purpose of obtaining something in return for the abductee's release. This is typically a ransom payment, though perpetrators may demand political concessions. In some cases, what may ostensibly be a political cause may, in fact, be extortion.

The term 'hostage-taking' is used to describe a situation where the location of the abductee is known and their release depends on the fulfilment of specific demands. In a siege situation the perpetrators and their hostages have been located and surrounded by security forces, and the perpetrators threaten to kill hostages unless they are given a means of escape.

Types of kidnappings

- **Ransom kidnapping** – where the primary motive is financial or political gain. The kidnappers demand a ransom from the abductee's family or associates in exchange for their release. The kidnappers may also demand the release of prisoners, policy changes or publicity for their cause.
- **Express kidnapping** – where the victim is held for a short period, typically less than 24 hours, and forced to provide a quick ransom payment (e.g. by withdrawing money from an ATM). Express kidnappings are generally opportunistic and will not have involved much planning.

- **Virtual kidnapping** – where criminals attempt to coerce victims into paying a ransom by falsely claiming they have kidnapped someone they know. Tactics include keeping the victim on the phone to prevent them from verifying the person's safety or the authenticity of any audio or video recording of the supposed victim. This type of kidnapping has been aided in recent years by new technologies, notably AI.
- **Tiger kidnapping** – where people known to a target are abducted, and the target is forced to participate in a crime, such as accessing a secure location to steal cash, to ensure their safe release.

7.9.2 Planning, preparation and training

To contend with the threat of abduction, organisations need to assess who is most at risk and tailor their risk mitigation and preparedness measures to the context. Regular training, simulation exercises, appropriate resourcing, continuous learning and adaptability are essential for both prevention and response. Example actions are outlined below.

At the head office level

- Establishing and maintaining up-to-date security policies and protocols specifically addressing abduction risks – and ensuring that all staff members are aware of these policies and receive orientation.
- Creating an organisational crisis management structure with relevant staff selection and training.

▶ *To learn more about the crisis management structure see Chapter 4.4.*

- Establishing links locally and internationally to ensure expertise for effective incident management support as and when required. For example, discussing what government help can be expected if a staff member is abducted or identifying qualified external experts for crisis management and post-crisis support to abductees and their families.[115]
- Keeping staff records up to date, including the contact details of close relatives and any medical conditions. Consider having all staff document 'proof of life' questions (see more on this below).

115 There are several specialised response organisations that will support organisations and families throughout abduction events, with many associated with special insurance policies. Some governments maintain dedicated law enforcement teams to engage if one of their citizens is involved in an abduction.

- Being clear about responsibilities and obligations to staff and their families in the case of abduction – including where staff are seconded.
- Fully informing staff of the abduction risk before assigning them to high-risk areas.
- Preparing templates or guidelines for media statements and press releases in case of an abduction.
- Training staff on abduction risk mitigation strategies and how to survive an abduction.
- Ensuring that insurance policies are in place, including medical insurance, and special risks or kidnap and ransom insurance.

At the operational office level

- Ensuring there is a staffed and trained organisational crisis management structure in place.
- Ensuring awareness of the organisation's kidnap and ransom policy and that staff are prepared to respond to abductions (including calls from kidnappers).
- Developing abduction-specific contingency plans and regularly reviewing and updating these and standard operating procedures.
- Establishing and maintaining effective and reliable communication channels to report incidents and share notifications during the management of a critical incident.
- Establishing and maintaining contact with relevant embassies (if abductees are foreign nationals) and other diplomatic actors, such as the UN, in coordination with the country's crisis management team.
- Knowing who to contact in the government in the event of an abduction and, if there are specialist teams, investing time in understanding how they operate and respond.
- Being informed about the command structure of the national security forces and other relevant armed actors in the organisation's area of operation.
- Understanding government policy on contact with perpetrators – entering into direct negotiations with perpetrators could have serious consequences.
- Ensuring that clear records are kept and maintaining confidentiality. These records should be marked as 'Privileged', and staff should expect that the records may at some point be called for as part of an enquiry.
- Being prepared to provide psychosocial support to affected staff and their families and address trauma and stress-related issues.

▶ *See Chapter 5.4 for more details on staff care following a critical incident.*

Kidnap, ransom and extortion insurance

Kidnap, ransom and extortion insurance is specifically designed to protect individuals and organisations against associated financial losses and liabilities.

While terms and coverage vary by policy and insurer, kidnap and ransom insurance can provide:

- 'Preventative services', such as country-specific information and guidance.
- The provision of crisis response consultants who can offer negotiation support and strategic advice.
- Cover for lawsuits, public relations, rest and rehabilitation expenses, medical and psychiatric care, personal accident compensation, loss of income and any other related legal liabilities. It might also cover ransom reimbursement if this is not illegal in the relevant jurisdiction (for example, if perpetrators are sanctioned groups or individuals).

Kidnap, ransom and extortion insurance usually includes a confidentiality clause, with only senior management being briefed on policy details. It is important that organisations can discuss the insurance plan with staff without compromising this. Organisations can develop a statement and nominate a spokesperson in case of enquiry.

Some insurance plans allow for 10% of the annual premium to be deducted for preparation and training.

▶ *See Chapter 5.4 for more details on insurance.*

7.9.3 Risk reduction measures

The following are examples of measures to reduce abduction risks.

- **Context awareness.** Gathering information on the security context and abduction risks through, for example, security information monitoring, attending context-specific security briefings and understanding the measures adopted by other organisations operating in the same area.
- **Communication and acceptance.** Discussing the organisation's role and work with relevant actors while ensuring high programme quality and acceptance.
- **Avoiding predictability.** Varying routines and travel times, including on commutes and outside of work.
- **Reducing visibility.** Minimising visibility by evaluating branding such as logos on vehicles, being aware of behaviour that might attract attention, using trusted transport rather than identifiable vehicles for some travel, operating in smaller teams and limiting social media presence.
- **Following operating procedures.** Using secure communication channels for sensitive information, ensuring travel risk management measures are in place and followed and maintaining up-to-date contingency plans for unexpected situations.
- **Removing potential vulnerabilities**. Temporarily restricting access to high-risk areas, asking staff to work remotely and considering the suspension of programmes are strategies to consider when there is evidence to suggest heightened risk. Some organisations find it useful to have staff travel with temporary, 'clean' work-related devices such as phones and laptops to prevent the misuse of any stored data. A more drastic measure is to withdraw staff at highest risk.
- **Site security.** Implementing strict access controls and identification procedures at residences, offices and project locations. While abductions often occur when in transit, maintaining secure sites remains crucial.

▶ *See Chapter 7.2 – Site security.*

- **Heightened awareness and anti-surveillance.** Being vigilant (collectively and individually) about any signs of surveillance and unusual behaviour. An abduction normally involves planning, and the perpetrators may be watching the residence, office and movements of their target for some time before making their move. Regular training on reporting protocols and anti-surveillance practices is recommended.

▶ *See Chapter 7.5 for more information on hostile surveillance.*

- **Using technology**. Digital tracking equipment can be carried personally or installed in vehicles, allowing for digital alerts and route tracking. Digital tracking equipment should be used with caution and assessed for security risks.
- **Local support and protection.** Building and maintaining good relationships with community leaders and local authorities can help provide access to advice on security measures and potential abduction risks. In some contexts it might also afford some protection. However, power dynamics can shift rapidly, and careful consideration needs to be given to this before or when seeking such support.
- **Armed protection.** Using armed guards or bodyguards can be a deterrent for would-be perpetrators at residences, offices and during travel. However, the use of armed protection can also increase visibility and heighten risk for both the armed personnel and staff. This needs to be carefully evaluated in light of the organisation's policies, principles, image and acceptance measures. It is also critical to consider sanctions and counter-terrorism legislation when using armed protection.

▶ *See Chapter 4.2 for a more detailed discussion on armed protection.*

- **Public policy of 'no ransom' or other substantial concessions.** Taking a stance on ransoms in policy documents and public communications can make staff less attractive targets. In reality, some money is sometimes paid – by families, private companies, governments and aid organisations. A 'non-payment' strategy is difficult to maintain without sustained preparedness at all levels of an organisation and a high level of community contact and connections with a wide range of stakeholders.

Mitigating express and virtual kidnapping risks

Express kidnappings are usually financially motivated, and kidnappers do not intend to physically harm their targets. Some of the following steps can help mitigate the risks:

- Conducting risk assessments (high-risk areas, likely targets, impact).
- Training staff on situational awareness, how to avoid becoming a target (guidance around ATM use) and responding appropriately for safe release (complying with demands).

- Carrying limited (minimal) valuables and bank cards with low balances or daily withdrawal limits.

Virtual kidnappings are designed to get money quickly. Mitigation measures include:

- Training staff on the existence of AI-generated deep fakes and how to identify signs that this is a virtual kidnapping (such as perpetrators trying to keep the target on the call, blocking their efforts to contact/speak to the supposed victim, and rapidly lowering ransom demands).
- Training staff to respond calmly – hang up, contact the supposed victim or ask for details only they would know.
- Ensuring staff are aware that they should not agree to pay a ransom, especially in person, as this could place them at further risk.

7.9.4 Responding to an incident

General response considerations

When an abduction occurs, the organisation will typically activate its crisis management structure. Larger organisations may have a crisis management team at the head office level, supported by an incident management team at the operational office or incident site. International organisations might also have a regional crisis management team. These teams are usually supported by colleagues with a broad range of expertise, often from security, health, IT and communications. The organisation will usually identify a designated communicator to convey messages to and from the perpetrators. (This role is not the same as a negotiator, and this individual will not act as a decision-maker or a formal member of a response team.) Response teams often work with other organisations, such as law enforcement, government agencies, the media and insurance companies.

A key responsibility of the crisis management team is to develop and implement a tailored incident response strategy, adjusted as circumstances evolve. This strategy, informed by experts such as legal counsel, helps ensure compliance with relevant legal frameworks and guides the organisation's approach to the

response, including negotiations with perpetrators, stakeholder management and communications. Strategies towards perpetrators, relatives, authorities, media and other organisations will need to be regularly reviewed by the crisis management team.

▶ *See Chapter 4.4 for more good practice on how to respond to critical incidents and establish a crisis management structure.*

Actions during the initial phases of a suspected abduction can include:

- Establishing the facts and preparing an incident report.
- Ensuring the safety of other staff, perhaps restricting their movements or moving them to a more secure location.
- Considering whether programmes should be suspended.
- Informing other offices and senior management.
- Informing family members and preparing them for potential contact from the perpetrators.
- Alerting insurance companies.
- Consulting relevant external expertise, in line with the crisis management plan.
- Managing communications and information including setting up a logbook to record events, discussions, decisions, responsibilities and actions taken at all relevant office locations.
- Identifying the designated communicator.
- Monitoring the media for information relating to the incident.
- Ensuring financial readiness to cover initial costs, which may require securing funds from head office.

During the initial stages of an abduction, response staff will often need to be relieved of other duties and provided with a dedicated workspace and facilities. Team members will need regular rest and support, and if the crisis extends for a long period, a smooth handover to alternates.

Outside experts

In some cases, a specialist in abduction situations may join the crisis management team from outside the organisation, such as from the host or home government, the insurance company or a private security firm. Their role is to advise and support, not to make decisions. Experts in abduction management might come forward voluntarily or they might be recommended. Their knowledge of the local and regional context and their understanding of the legalities – as well as their capabilities, networks and experience – can be invaluable.

While external advisors do not generally manage an incident or engage in direct negotiations with perpetrators, they can add significant value when acting as advisors and coaches to staff, such as the response and media teams. They can offer an objective perspective, help anticipate possible scenarios, help ensure response readiness and evaluate response effectiveness. Care needs to be taken to ensure no conflict of interest arises – for example, in the case of a government-recommended or -appointed expert, there may be misalignment in terms of policies, goals and approaches.

Where staff from multiple organisations are abducted together, collaboration among the different concerned parties is essential to ensure a unified approach. Joint crisis management teams at operational and head office levels are advisable. While each organisation will want to be involved, team members must be chosen for their skill and competence in managing incidents, rather than as representatives of their respective organisations. Outside experts may be brought in to maintain objectivity and focus.

Even when an incident affects only one organisation, there may be implications for the security of others in the same area. There is, therefore, a collective responsibility for security. Payment of a ransom or how an organisation interacts with authorities also has broader security implications. While an organisation whose staff member has been abducted is responsible for choosing the

approach it wants to take, it may still be prudent to listen to advice from others with experience in the area, especially if they have experienced similar situations.

When the whereabouts of the abductee are unknown

An abduction will be especially challenging when the whereabouts and status of the abducted individual are unknown, and if it is impossible to contact the perpetrators. The targeted organisation may seek to generate publicity about the incident, but as with any media engagement this may be counterproductive if it unnecessarily raises the profile of the abductee and heightens their value to the perpetrators. Alternatively, this may be a good approach if it signals to the authorities that there is widespread awareness of the fate of the person concerned and that their continued abduction would seriously damage the image of the authorities and their capacity to establish or maintain the rule of law. Human rights and other advocacy organisations are generally better at creating this type of publicity than humanitarian organisations, and it may be possible to cooperate with them. In other cases, there may be little that can be done beyond circulating information and pictures of the abductee, and trying to find someone who can provide a lead or a contact.

Managing relations with the family

- **Immediate contact and family liaison.** Informing the abductee's family promptly is crucial – preferably in person and ideally before they learn of the incident through the media or other third parties. An in-person visit is recommended. Dedicated family liaison functions are advisable. Those in family liaison roles – whether internal or outsourced to specialists[116] – can help to build and maintain trust, and should have strong interpersonal skills and be able to communicate in the family's language. Some governments also have family liaison officers; these should supplement rather than replace organisational engagement.

  In some instances, families, particularly if they are local to the context, might prefer to manage abductions themselves drawing on local knowledge and networks, especially if local social or political rivalries drive the abduction.

116 If an organisation does not have a dedicated or trained family liaison, prior arrangements for support can be made with specialist organisations such as Hostage International: www.hostageinternational.org

However, in criminal or politically motivated cases they may not be better equipped than the organisation. Sometimes staff may be abducted for reasons unrelated to their work, and some organisations may choose not to intervene unless directly implicated. In these circumstances, it is important that the family and the organisation understand and agree on the response strategy and where mutual support may be possible.

- **Developing a clear approach.** Maintaining transparent communication with the family is essential to fostering trust. A lack of trust can lead to the family acting independently – for example going to the media, visiting the location where the abduction took place or attempting their own negotiations. The family will also be more prepared than the organisation to pay a ransom and may start selling assets to collect the money. While families have their own right of initiative, organisations should guide them on the potential consequences and risks of such actions. Paying a ransom does not guarantee release and may lead to further demands.
- **Managing the disclosure of information.** Sharing information with family members and others has to be carefully balanced with the need to effectively manage the incident.

▶ *See Chapter 4.4 for more on family liaison.*

Liaising with authorities

It is advisable to inform the authorities – relevant government departments and institutions – immediately about an abduction. This includes authorities in the country where the abduction took place, as well as the government of the country of the abductee (this may involve several authorities if they hold more than one nationality). Even if the abduction occurs in a non-government-controlled area, the government should still be notified.

The crisis management team will need to decide on a policy and how to leverage relations with all relevant authorities. Authorities will have access to information and intelligence, networks and services that may not be available to the organisation and, therefore, may be in the best position to support a release. This is especially the case for authorities in the country where the abduction took place. At the same time, the authorities may have an agenda that is not in the direct interest and wellbeing of the abductee. They may also be mistrustful of the capacity of an aid organisation to handle the abduction properly, or may want to prevent the organisation from entering into dialogue with perpetrators who they may regard as 'terrorists' or rebels (in some countries, contact may be illegal).

If the authorities are keen to bring the incident to a rapid conclusion, they may be predisposed to use force instead of, or in conjunction with, any negotiations.

Practicalities and principles to be agreed and confirmed with relevant authorities may include:

- The security, safety and wellbeing of the abductee should be the primary concern.
- The overall response strategy.
- The media strategy (including confidentiality).
- A joint approach to the family – collaboration with any government family liaison officers is beneficial.
- The choice of a communicator (see below).

Some organisations have embedded a staff member in a government response management team. Under such an arrangement, it is important that the organisational representative understands the organisation's position and the boundaries of the relationship.

Guidance for initial contact with the local authorities

- Discuss and agree within the different response teams the line to be taken.
- Prepare a script to inform the authorities of the facts.
- Get in touch with a formal contact, who should already be known.
- Leverage all means to ensure that the security of the abductee is the top priority.
- Anticipate that, once briefed, the authorities may contact and liaise with the media.
- Establish a contact procedure for future briefings.

▶ *See Chapter 4.4 for more on liaising with authorities during crises.*

Managing communications

Managing communication effectively during an abduction involves strategic planning, maintaining confidentiality and coordinating with both internal and external stakeholders to ensure the safety and wellbeing of the abductee and their family.

Sharing details outside the organisation should be carefully assessed, and should only occur as part of a deliberate plan aimed at supporting release. Adopting a 'need-to-know' basis for information sharing is considered good practice.

It is advisable for the crisis management team to decide on communications with internal and external stakeholders, supported by a crisis communications team. The crisis communications team would be responsible for managing media relations, including crafting and implementing communication strategies, monitoring media and appointing a spokesperson. They may also assist in protecting the privacy of the abductee and their family by managing social media. Shutting down social media accounts may be advisable to stop perpetrators from accessing them.

Keeping messages clear and concise helps in managing media coverage. A central message can emphasise that the organisation holds the perpetrators accountable for the staff member's safety and wellbeing, and that all that can be done is being done. Given that different media (international and national) may present the story differently, it is essential that media staff in different offices consult each other before issuing any organisational statements.

To manage media inquiries and public interest, the organisation can post updates on its website. This helps reduce phone inquiries and ensures consistent messaging. Organisations should assume that the perpetrators are monitoring the news, making it unwise to attempt communication or negotiation through public media channels. Media messages can easily become distorted, undermining genuine communication and negotiation efforts. It is important to engage with editors and journalists to encourage collaboration.

If the family wishes to make a public appeal, this should be done constructively and managed carefully. The target audience is usually not the perpetrators but the authorities responsible for security, with messages crafted to ensure continued efforts to resolve the situation.

Case example: Controlling rumour

During the final phase of negotiations for the release of abducted aid workers in Somalia, controlling rumours became a real challenge. While the situation was still tense, another aid organisation unexpectedly announced that the abductees had been released and had left on a plane the previous day. This rumour circulated immediately within the aid community and was taken up by the local media. It took the organisation involved in the kidnapping two frantic hours to find out where the announcement had come from, and to issue a correction.

Publicity can be beneficial if the perpetrators are sensitive to their reputation, though this is rarely the case for groups that use abductions to garner attention. In such cases, perpetrators can engage the media themselves, transforming the situation into a dangerous spectacle where the abductee's death may be used to create a dramatic climax. Countering this requires persuading the media not to participate in sensationalising the situation.

When there is a possibility that abductees have access to media, sending supportive messages through these channels can help boost their morale.

Effective internal communication – such as through briefings or intranet posts – can help staff feel included and informed in a way that supports and reinforces the formal response effort. Sometimes staff establish voluntary appeal funds to support the family of the abductee.

► *For more on communication and crisis management see Chapter 4.4.*

Ransom

In principle no ransom should ever be paid, as this increases the general risk of repeat or copycat incidents targeting the same organisation or others in the area. The reality is that, in many cases, some ransom or concession is paid, though organisations may deny this.

Where paying a ransom is a viable potential strategy, a comprehensive legal and political analysis should be conducted beforehand to help identify any potential

legal or financial implications and risks (across all relevant jurisdictions: the country where the incident occurred, the home country of the organisation and the home country of the abductee). That said, political considerations can impact whether a government will enforce this legislation. Organisations should also be aware that, even if they have insurance that covers ransom payments, these are reimbursed afterwards, and therefore the organisation will have to ensure it has the necessary funds to hand to make the payment in the first instance.

7.9.5 Negotiations and communications

Communicating and negotiating with the perpetrators

A critical element in the negotiations will be the demands made by the perpetrators – and the question of who, in practice, can or should meet them. Perpetrators' objectives and demands can change. There are many examples of situations where political demands withered away, leaving only a demand for money. The reverse can also be true: a criminal gang may 'sell on' an abductee to a politically motivated group if no ransom is forthcoming. If the perpetrators ask for political concessions from authorities, this will be beyond the organisation's control.

Guidance for initial contact with perpetrators

- Ensure that a communicator is briefed and has a script for contact; this will need to be in relevant languages.
- Always record the conversation. This may require separate equipment (e.g. a smartphone).
- Adopt a cooperative attitude.
- Ask to speak to the abductee.
- Insist on proof that the abductee is alive.
- Explain the limited responsibilities of the communicator (see below).
- Set a deadline for a reply.
- Establish a procedure for return calls (e.g. telephone number, code word).
- Once contact is established, prepare a revised script for subsequent interactions.

Good practice for communicating with perpetrators includes the following.

- Recording and logging all details and scripts relating to calls with perpetrators. These must remain confidential.
- Assessing the motivations of the perpetrators and determining if their behaviour follows a consistent pattern over time. Are they aggressive and threatening, rational and factual, or highly emotional? What tone and communication style would be most effective in de-escalating the situation and building rapport?
- Requesting proof of identity and possession to confirm that the abductee is still alive and has not been transferred to another group. While a tape or video recording can be helpful, it is not definitive proof of life – especially given the rise in the use of AI (which can replicate voices and videos). The organisation should ask for a specific, intimate detail from the family or a close friend – something the perpetrators are unlikely to know. Proof of life questions can also be used if on record. If no credible proof of identity and life is provided, organisations should consider discontinuing negotiations.

Proof of life

Establishing proof that an abductee is still alive is critical, and organisations should consider mandating proof of life questions as part of next of kin information. Care should be taken as to how this information is stored and transmitted. As soon as possible, additional proof of life questions should be obtained from the family to allow the organisation to continue checking this as the incident progresses. These questions must be unique and easy for the abductee to answer.

- Referring to the abductee by name whenever possible to humanise them in the eyes of the perpetrator and encourage good treatment, including indicating any special needs they may have, for example wearing glasses or taking medication. Signalling other concerns, such as the emotional state of family and children, and exploring whether a way can be found to arrange an exchange of messages, can be beneficial.

- Emphasising that the communicator has no decision-making authority and needs to consult with others. This provides time to think and gives the organisation some room for manoeuvre. At the same time, no indication should be given that a third party (the authorities or a crisis response expert, for instance) is advising the organisation. Preparation is needed in the event perpetrators demand to speak with the decision-maker rather than the communicator.
- Restating the no ransom policy to show that the organisation remains consistent and that the passage of time is not weakening its resolve.
- Agreeing communication times and methods, building in contingencies for issues such as poor mobile coverage and network disruption. This includes establishing a code word with the perpetrators to confirm their identity, ensuring that the organisation is not communicating with impostors.
- Sustaining the communication. Organisations should not break contact with the perpetrators unless there is certainty that the person they are speaking with is not the real perpetrator or that the abductee is no longer alive. The perpetrators should know that the organisation is keen to maintain communication.
- Not agreeing to go to a specified place for an encounter. If there is very strong pressure to do so, the organisation should insist on detailed guarantees of safety. There is a risk of further abductions.

At some point, the organisation's communicator may talk directly to the abducted staff member, and it is important to be clear on what kind of information and messages should be passed on. The communicator should try to avoid providing the abductee with any information that the perpetrators should not know, but reassure them that everything possible is being done to secure their release. Often abductees worry about how their family is coping, and the communicator can try to alleviate this concern.

The role of the communicator

The designation of 'communicator' is deliberately distinct from 'negotiator' as the crisis management team should retain control over any negotiations. Designating a communicator in the initial phases can also serve to create a time lag to allow for internal and external consultation and analysis before responding to perpetrators' demands and adds to the communicator's position that they are not able to make decisions. These individuals should be well rehearsed and supported as they communicate directly with the perpetrators. They usually report directly to the senior decision-making authority of the crisis management

team. As abductions can last for a long time, more than one communicator may be required.

The communicator must be able to effectively manage high levels of stress while adhering to a negotiation strategy. This role may be filled by someone from the organisation or by an external expert. Ideally, the communicator would be a national who is fluent in the perpetrators' language and dialect, understands the culture, and has a solid grasp of the local dynamics and social interactions. They must be reliable and able to work under extreme pressure, available 24/7, and ready to follow instructions from the crisis management team. The communicator needs to be well trained, ideally through simulation exercises, as they are likely to face unexpected demands and pressures from the perpetrators.

Communicators are not members of the crisis management team and are not involved in regular crisis management team meetings. This is to avoid them knowing too much and accidentally disclosing important information to perpetrators. If the perpetrators demand to speak with someone other than the designated communicator, the organisation should ensure that the preferred communicator listens discreetly to the conversation.

Communicators may also be from outside the organisation. An intermediary can come forward from within the community, or one can be sought out by the organisation, proposed or approached by the authorities or even put forward by the perpetrators. It is not uncommon for locally respected and influential people to involve themselves in abduction resolution – elders have played an influential role in Somalia and Afghanistan, for example.

In a situation of high acceptance, and where the community retains a measure of influence over the perpetrators, a trustworthy individual from the local community may be able to secure the release of the abductee. It should be made clear, however, that they cannot make commitments on the organisation's behalf without its prior consent. In the face of well-organised criminals who are more autonomous from the community, traditional leaders may be ineffective. The question of trust is crucial. On whose behalf is the intermediary acting? Do they have connections with the perpetrators? Who controls the negotiations? There will also be a question of payment. Organisations may need to consider reimbursing some operating expenses for local intermediaries, for instance to cover travel, accommodation, food and communications. Such payment, however, may not be appropriate if the organisation is dealing with a person who, in local terms, is known to be relatively wealthy already.

The authorities may also put forward an official negotiator. The negotiator's first step will likely be to establish a climate for dialogue. Initially, the focus will probably be on minor issues on which agreement can be reached. This will establish a basis for discussion of more difficult issues. If the authorities provide the negotiator, there is a risk that considerations other than a concern for the safety and release of the abductee will come into play. Alternatively, a prestigious non-governmental entity may propose an envoy to try to mediate the release.

Obtaining release by force

It is not uncommon for security forces to try to locate the abductee and attempt a rescue or to create a siege situation to force the perpetrators to surrender. This is a high-risk strategy for the abductee. There are several ways forced release scenarios can go wrong, with potentially fatal results.

From the organisation's point of view, two elements are particularly important.

- Do those carrying out the action have a clear overall command? If they do not, uncoordinated actions could imperil the life of the abductee.
- Do troops have a clear description of the abductee in order to be able to differentiate them from the perpetrators, and have they been given clear instructions only to fire on those firing at them? The abductee may be wearing the same kind of clothes as their perpetrators and can be harmed in the confusion of a siege.

In reality, the ability of the family or the organisation to influence the plans and actions of security forces may be limited. Authorities will respond as they see fit, and direct action by any authority is likely to be kept a secret for operational security reasons.

Responding to sudden siege situations

Some siege situations may happen suddenly and be largely out of the organisation's control. An example includes the 2015 siege of the Radisson Blu hotel in Mali, where aid workers were among the hostages taken. While armed forces will lead the response to these situations, organisations can aim to:

- Quickly ascertain if any staff members have been affected by the incident.

- Implement measures to protect remaining staff, such as relocating them from the area.
- Mobilise crisis management teams to handle family liaison, manage media relations and coordinate with authorities.
- Be prepared to provide support to affected staff, including medical and psychological care, insurance payments and repatriation.
- Conduct an after-action review to assess the effectiveness of pre-incident security measures and the organisation's response, sharing the findings with relevant staff.

7.9.6 Managing the aftermath

An abduction may conclude with the release or death of the abductee – or, in some cases, remain unresolved indefinitely. Aid organisations need to be prepared to manage a range of possible outcomes.

Release

The return of released individuals needs to be properly organised and managed. During initial release, survivors should be received by someone they know, perhaps a close colleague. A female colleague would be best when the abductee is also female. As a priority, their immediate physical needs and comfort will need to be addressed.

If multiple staff from different organisations were involved in the abduction, then the situation might not be resolved for all stakeholders. If this is the case, extreme care needs to be taken with public statements until the incident is resolved for all parties.

Good practice considerations include:

- Attending to the needs of the survivor and their family members, both immediately and in the longer term.
- Informing and following up with relevant stakeholders, such as the media, other organisations and authorities, and managing their interactions with, and access to, the survivor.
- Debriefing the survivor when they are ready.
- Following up with individuals and groups who supported the response.

- Providing support, such as time off, for response team members.
- Deactivating the crisis management structure, including filing records and documents, and producing a final incident report that can be shared with internal and external stakeholders.

Abductions can be traumatic experiences. Survivors may need long-term help and access to professional support, especially during the initial phases. The organisation should take every possible measure to reduce the burden placed on survivors and allow them to recover.

It is good practice to bring survivors into decision-making directly affecting them – following a survivor-centred approach – but to do so progressively and in line with medical advice and the individual's own wishes.

▶ *For more details see Chapter 5.4 on staff care.*

Unsuccessful resolution

An unsuccessful resolution may involve confirmed death with the body recovered, notification of death with no body recovered, or the case is unresolved (such as if no proof of life is obtained or there is no contact from perpetrators).

It is advisable for organisations to be prepared to provide long-term support to the family and other staff affected by the incident.

▶ *For more details on what this support might include, see Chapter 5.4 on staff care.*

In the event a body is recovered, an autopsy and investigation will likely be required either in the country where the incident took place or elsewhere. There may also be a formal coroner's enquiry (or inquest) in the abductee's home country. Organisations need to be prepared to cooperate with the authorities and share evidence.

The family may also question how the organisation handled the incident, initiate an inquiry and take legal action against it. In this case, the records the organisation kept as the incident unfolded will be an important source of evidence.

If things go wrong in an abduction managed by the authorities, the organisation may request an inquiry into how the operation was conducted and whether what went wrong could have been avoided.

After-action reviews

After-action reviews focus on what happened and why: the decisions made, why they were made and what the outcomes were. An after-action review can include accountability elements but should not be an exercise in assigning blame. The review should aim to identify what actions can be taken to avoid similar incidents in the future, and how to manage them if they do occur.

It is important for an organisation to be transparent about its findings – especially with staff affected by the incident. The review can be disseminated through a session where key stakeholders, including the survivor, are invited to share lessons learned. Failure by the Norwegian Refugee Council to share information openly with affected staff was identified as a shortcoming during the court case following the abduction of staff members in Dadaab, Kenya, in 2012.

► *For more details on after-action reviews see Chapter 4.4.*

Further information

Guidance and resources

Buth, P. (2010) *Crisis management of critical incidents.* EISF (www.gisf.ngo/resource/crisis-management-of-critical-incidents).

Clamp, D. (2022) *Ten years on: learning from the Steve Dennis case.* GISF (www.gisf.ngo/blogs/ten-years-on-learning-from-the-steve-dennis-case/).

Davidson, S. (2013) *Managing the message. Communication and media management in a security crisis.* EISF (www.gisf.ngo/resource/managing-the-message).

EISF (2017) *Abduction and kidnap risk management guide* (www.gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

Hostage International (n.d.a) *How we can help* (www.hostageinternational.org/how-we-can-help/).

Hostage US (2022) *A life after captivity. Reintegration guide* (www.gisf.ngo/resource/a-life-after-captivity/).

Hostage US (n.d.) *Hostage US guides* (https://hostageus.org/resources/hostage-us-guides).

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

7.10 Combat-related threats and remnants of war

This chapter considers threats emanating from major armed conflict or 'acts of terror', including bombing, missiles and shelling, crossfire and sniper fire, improvised explosive devices (IEDs) and chemical, biological, radiological and nuclear (CBRN) weapons. It also includes a discussion of siege tactics and the dangers of 'remnants of war' such as landmines and unexploded ordnance (UXO). The chapter presents mitigation measures for organisations to consider, but for extreme environments involving major combat, the good practice guidance in this volume will not be sufficient, and cannot take the place of direct consultation with experts.

7.10.1 Core questions and considerations

The first issues to consider in active combat areas are whether the organisation is willing and has the capacity to operate under these conditions, and whether the benefits of doing so (i.e. programme criticality) outweigh the residual risks. Are there significant assistance and/or protection needs – and opportunities to meet them – that warrant the organisation's presence? How many and what sort of staff will be required to effectively fulfil this function? What additional inputs – including training, equipment, specialised skills and insurance – will be needed to meet duty of care obligations?

The reality is that, in most areas of active combat, the humanitarian presence, especially of international organisations, will be far lower than in low-level conflict or non-conflict settings. Along with other civilians, humanitarians are at risk of collateral violence (and of direct targeting by armed actors), for which security risk management efforts can do little beyond avoiding the highest-risk locations and adopting sheltering protocols. For most organisations, the costs and capacities required to mitigate the risks to staff in major active armed conflicts are prohibitive, and those who choose to operate will often programme in safer areas and focus on displaced populations and adjacent needs.

The risk to organisations in combat settings is not always limited to collateral violence. There have been numerous instances of direct targeting of humanitarian actors and operations by national militaries as well as non-state armed groups. Organisations that are comfortable mitigating risks of collateral

violence will usually draw the line at operating where there is a high risk of direct targeting, and where efforts at acceptance and negotiated access are insufficient to mitigate these risks. In these circumstances informal, local volunteer groups and individuals – who have even less ability to protect themselves – are often the primary aid providers.[117] This leads to another core question: if an organisation supports these ad hoc efforts through sub-grants or other means, how well is it helping to mitigate the risks of its partners?

Finally, even though only a small proportion of humanitarian organisations elect to work in the most extreme high-risk areas, coordination and communication in these contexts is more vital than ever. In these settings, organisations should endeavour to seek out, support and participate in collective action efforts on deconfliction, humanitarian access and advocacy for the protection and safe passage of aid.

7.10.2 General mitigation measures for combat zones

Organisations intending to operate in areas of active combat, where they may face direct or collateral violence from air strikes and/or heavy munitions (bombing, shelling, landmines or grenades, for example), should include the following general considerations in their security risk management planning.

Risk assessments and mitigation measures

Combat-related threats should be carefully considered in risk assessments. Specialist input may be required to identify and implement mitigation measures (examples are given below). Crisis management structures and up-to-date contingency plans are particularly important in areas of active conflict. Organisations benefit from having a system in place to monitor security levels and adapt security risk management measures when there is a transition from non-conflict to conflict (or vice versa), which might happen slowly or suddenly.[118] The higher the risk, the greater the organisation's duty of care. This means that the most at-risk staff must be identified and provided with the highest level of security risk management support. Organisations should also consider how to support partners who may be implementing on their behalf in these contexts.

▶ *See Chapter 3.5 on partnerships.*

117 See 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).

118 For a fuller discussion, see GISF and Humanitarian Outcomes (2024).

Location selection

The location of staff and assets is usually the first consideration, and should be informed by the risk assessment and context analysis. Offices, warehouses and residences should be sited away from obvious or likely military targets, such as airfields, barracks, fuel depots, official buildings or strategic points such as crossroads, railheads, power stations and radio and TV buildings. If the organisation is working in an area likely to come under fire, its facilities should be moved as far away as operational requirements permit. First and second fall-back locations can be identified in advance in case violence intensifies in, or spreads from, the target area.

Recruitment and staffing

Ideally, humanitarian staff working in combat-affected areas, especially those with security responsibilities, will have both prior experience in comparable environments and specialised training in relevant areas of security risk management. They should ideally also demonstrate good judgement, the ability to work under pressure and mental resilience. Recruitment, always a challenge in humanitarian aid, is even more so for operations amid armed conflict. These settings require more investment both in security risk management and in staff care in general, including rest and recuperation (R&R) allowances and mental health support. To reduce stigma and encourage more staff to avail themselves of them, mental health services can be provided to all staff on an opt-out basis, rather than on request.

▶ *See Chapter 5.4 for more on staff care.*

Training

It is good practice to ensure staff are trained in SOPs and what to do in the event of a serious incident or increase in violence. Staff training in preparation for working in active combat areas should include situational awareness, first aid, use of personal protective equipment (PPE) and other relevant equipment, evacuation and sheltering procedures, what to do under fire and stress and psychological first aid.

▶ *See Chapter 5.2 for more on training.*

▶ *See Chapter 5.5 for more on first aid.*

Deconfliction

Deconfliction efforts – such as the Humanitarian Notification System for Deconfliction (HNS4D) – provide information on an organisation's movements and static locations to military actors in an effort to avoid inadvertent strikes and collateral damage.

There may be cases where one or more armed actors are not participating in deconfliction, or are using the information for malign purposes. If the organisation knows that combatants are acting in bad faith and may be targeting humanitarians, a low-profile approach to locations and movements (including robust information security) may be advisable.

In cases where the organisation deems it safer to have a high profile and inform military actors of their presence, additional deconfliction measures could include painting the logo in bright colours on the roofs and walls of the organisation's buildings, marking vehicles, using special licence plates or using thermal reflective material visible to drones, anti-tank weapons and other weapon systems that use thermal imaging cameras. An organisation's flag may not be visible from a distance or on a windless day. It should not be assumed that all potential threat actors are familiar with a humanitarian organisation's name and logo, or even that organisation's purpose.

▶ *See Chapter 2.1 for more on deconfliction.*

Physical protection for sites

Mitigating the risks of active combat on organisational facilities (offices, residences and work sites) can be costly and may require specialist advice and support. Threats can include direct strikes or collateral damage from bombing, missiles or shelling, grenade attacks from outside the perimeter, armed raids and vehicle-borne explosives. In combat areas, facilities will usually require physical protection or fortification, and may need to be located close to appropriate shelter sites.

Fortification measures

Injuries in a blast event can be caused by primary fragmentation (pieces of the body or the casement of the explosive weapon) or secondary fragmentation (debris from the surrounding environment propelled by the blast wave, such as window glass). Despite their name, blast walls are designed to stop shrapnel and bullets – not necessarily the blast wave of a bomb. They can be made of concrete,

steel, sandbags, oil drums or boxes filled with earth, and are used to protect a building's doors and windows and the entrance route to a shelter.

Buffer rooms along the sides of a building may provide protection from blasts. Glass injuries can be reduced by applying fragmentation retention film, also known as shatter-resistant film or 'blast film', to the inside of the window. Note that fragmentation retention film applied to a window with double glazing is largely ineffective, as is fragmentation retention film applied to the outside of a window. Fragmentation retention film will also not stop shrapnel or bullets. While fragmentation retention film is designed to keep the glass together, it is not meant to keep it in its frame. In a large explosion, the entire windowpane could be propelled into the room. Keeping away from windows and having them open to prevent inward pressure are two simple mitigation measures. Securing or removing objects that may become hazardous projectiles, such as rubbish bins and flowerpots, can also help mitigate risks. While refitting buildings to withstand blast waves can be costly and time-consuming, reinforcing key areas like entrance lobbies, where a blast is more likely, may be a practical step.

Certain building characteristics can provide additional protection, although no one building will likely meet all requirements. Ideally, buildings should not connect directly to areas beyond the organisation's control, such as public roads. Main entrances should not be in direct line of fire from a space outside the organisation's control, and offices should be separated from warehouses or garages with vehicle access, and have their own security perimeter. A clearly defined outer perimeter with reduced access points can further secure the inner area of the site. Underground garages, which present significant risks in the event of a car bomb, may be best avoided, but if used access should be limited to staff. Vehicle access barriers may provide added protection. Parking and drop-off areas for visitors should be located outside the external perimeter.

Perimeter measures

Speed control measures along access roads leading to entry points can help prevent vehicles from accelerating and ramming into the building. Measures might include specialised equipment or, alternatively, gravel-filled barrels or large concrete pots with flowers or shrubs, securely chained together. If the outer perimeter is close to the building, additional stand-off measures, such as concrete blocks or pots, can be erected to minimise the impact of an explosion.

The further from the building a blast occurs, the less impact it has. While a distance of 30 metres between the building and any blast would be desirable,

this is often not feasible. It is advisable for staff and visitor entrances, as well as parking areas, to be separate. Staff vehicles, even within secured perimeters, should be checked in case a vehicle has been secretly loaded with explosives to be detonated by remote control, or a suicide bomber has requisitioned the vehicle. Vehicles and visitors authorised to enter the building at the outer perimeter should be searched.

An unobstructed space of at least 10 metres between the outer and inner perimeter is recommended. Movement corridors within this space can be designated to control traffic, with any unauthorised movements outside these corridors prompting an immediate response from security personnel. Inside the building, spaces accessible to visitors should ideally remain separate from staff-only areas. Screening measures for visitors (and possibly also staff) at the entrance, including bag searches, are recommended. Ideally the entrance or lobby will be spacious enough to accommodate checks without directly connecting to other parts of the building, in case a blast occurs in this area. Important assets, such as central computer systems, should be located deeper within the building's restricted areas, and should not be easily identifiable.

Sheltering measures

While physical fortification can reduce the damage from near-misses, such as the effects of blasts and shrapnel, it is less effective against direct hits – no shelter, even a concrete bunker, can offer complete protection from all weapons. The best protection often lies in immediate action, such as taking shelter or, if there is no prior warning, hitting the ground to reduce exposure to fragmentation. Underground shelters, such as basements or parking garages, generally provide the safest options, with reinforced rooms on the ground floor being the next best alternative. Shelters should be large enough to accommodate everyone in the building, along with essential equipment, and close enough to be reached quickly. Organisations should set a time limit for reaching the shelter, around one or two minutes. Staff who cannot reach a shelter in that time from their usual place of work will need their own shelter nearer at hand. If the authorities have identified or constructed public shelters, staff need to know where these are.

Refuge trenches and foxholes can provide cover against mortar shells and strafing by low-flying planes or helicopters. They should be deep (2 metres), narrow and large enough for up to four people. A good construction is an L-shaped small trench, with two entry and exit points. The top can be protected with logs and two layers of sandbags. These also need maintenance: rain can cause entrances to crumble and flood the trench. Staff should watch out for

snakes or other dangerous animals, which may make nests in trenches or foxholes.

▶ *For more general good practice around site security, see Chapter 7.2.*

Personal protective equipment

PPE is often required in areas of active combat, though keep in mind that protective gear is not a solution in itself but rather one element of security planning.

The choice of PPE depends on the specific threats in the area, balancing protection with mobility and comfort. While higher levels offer more protection, they also tend to be heavier and more restrictive and users will require some initial instruction. Efforts should be made to ensure that the PPE provided fits well and is wearable by all necessary staff – sometimes the available PPE is not designed for women and sizing may be limited. Vest and helmet covers should identify the humanitarian organisation to distinguish the wearer from combatants. In most circumstances, PPE should not be worn without this visibility (unless the organisation is a particular target), lest its wearer is mistaken for a military actor.

Body armour (ballistic vests) comes in various types and with various protection levels. Protection levels are typically rated according to US National Institute of Justice (NIJ) standards.[119] In the NIJ 0101.06 standard there are five protection levels, from IIA (lowest) to IV (highest). The jackets most commonly used by humanitarian aid workers operating in combat conditions are NIJ level IIIA soft armour vests, which protect against most handgun rounds, or level III plate carriers with hard armour inserts (front and side plates), which can protect against rifle rounds. Ballistic helmets (level III) protect against head injuries from bullets and fragmentation.

Armoured vehicles can provide good protection against some combat-related threats. Civilian armoured vehicles are constructed with reinforced materials like hardened steel, synthetic fibres and thick bullet-proof glass. The specific components used depend on the desired level of protection. They can offer protection from assaults and attacks, bullets and gunfire. Unless specifically designed as a mine-proof vehicle, they do not provide adequate protection from the blast and shrapnel of an anti-tank mine or a well-made roadside bomb. Armoured vehicles are significantly heavier than normal vehicles and very expensive. Given the additional weight and the resulting longer braking distance,

119 See https://nij.ojp.gov/library/publications/understanding-nij-010106-armor-protection-levels

special driver training is required. It can be difficult for non-experts to distinguish an armoured vehicle from a standard one. However, where it is known that an organisation is using armoured vehicles, this can affect how the organisation is perceived by the local population and armed actors; use should be in line with the organisation's security approaches in the context in question.

► *See Chapter 4.2 for more on security approaches.*

Defensive driving training for evasive action

Courses are available to train drivers on how to respond if a vehicle comes under close fire. The decision of whether to speed away or stop will depend on where the fire is coming from and the intended target. Generally, there is more protection inside the vehicle than outside, and driving away from the area while staying as low as possible is usually the best option – but every situation will be different.

If caught in crossfire while outside on foot, staff should immediately seek cover behind a solid object, staying low and moving to safety by crouching in the case of small arms fire. If caught in an artillery bombardment, they should hit the ground and stay prone.

7.10.3 Combat weapons and tactics

The weapons used in major conflict range widely in their scale, severity and lethality, and the potential for exposure to one or more of them in an operational area may be beyond the risk threshold of many humanitarian aid organisations. The following sections of this chapter describe each of them in more detail, along with possible mitigation measures. In general, for organisations working in active conflict areas, some important areas to consider and invest in include:

- awareness and early warning capabilities;
- immediate access to appropriate shelter or cover;
- evacuation plans and sheltering protocols;
- availability of PPE; and
- threat-specific training and drills, including trauma first aid training.

Table 25 outlines the categories and features of typical combat weapons used in major conflict.

Table 25 Overview of combat weapons

Weapon	Description
Aerial bombing	Bombs dropped from overflying aircraft (airstrikes). Includes traditional air-dropped bombs and modern glide bombs, which can travel up to 60km to the target.
Missiles/rockets	Self-propelled explosive weapon that can be guided to a precise target (guided missile) or simply aimed on a trajectory (rocket).
Drones (UAVs)	Unmanned aerial vehicles that can carry explosive payloads. Also used for surveillance and targeting.
Projectiles/mortars (shelling)	Firing artillery shells over a high arced trajectory to hit targets at a distance. Sometimes described as artillery projectiles or mortars.
Rocket-propelled grenades (RPGs)	Shoulder-fired anti-tank grenades capable of destroying armoured vehicles and fortified positions at close range.
Improvised explosive devices (IEDs)	An explosive weapon that can be placed in a location, carried/worn or delivered by a vehicle. Can be triggered remotely or on contact.
Small arms	Handheld firearms e.g. rifles and handguns.
Mines	Concealed explosive devices designed to be detonated by the presence, proximity or contact of a person or vehicle.
Unexploded ordnance (UXO)	Bombs, shells, grenades or other munitions that have been fired, dropped or launched but failed to detonate.
White phosphorus	A toxic substance used for smokescreens that can be delivered by artillery shells, rockets and grenades.
Chemical, biological, radiological and nuclear (CBRN) weapons	Bombs and other weapos or tactics that use biological or chemical substances, radiation or nuclear explosions to cause death and/or toxic hazards.

Bombing from aerial platforms

When dealing with the threat of collateral violence from airstrikes, it is important to remember that high-risk locations are those anywhere in the proximity of high-value targets, where destruction would be militarily advantageous. Common targets of airstrikes include military installations, airfields, power stations, communication towers, bridges, key road junctions, transportation

systems and even, increasingly, hospitals. Weapons used for aerial bombing include missiles and drones.

Missiles vary in range, accuracy and speed, which can impact the effectiveness of alert systems and the time available to take shelter. Missiles have internal guidance systems that allow them to be directed or steered towards a specific target after launch.

- Ballistic missiles travel at hypersonic speeds during most of their flight, with intercontinental ballistic missiles (ICBMs) reaching targets in about 30 minutes. Their precision has improved significantly, with some modern systems achieving accuracy within tens of metres. They can carry very large payloads, often measured in thousands of kilograms, giving them immense destructive capacity.
- Cruise missiles typically fly lower and slower, with approach times measured in hours for long-range missions. While their warheads are generally smaller than ballistic missiles, modern cruise missiles can carry payloads of several hundred kilograms.
- Air-launched ballistic missiles, like Russia's Kinzhal, can achieve hypersonic speeds like ballistic missiles, resulting in short approach times, but can manoeuvre during flight. They typically carry payloads larger than cruise missiles, but smaller than traditional ballistic missiles.

Drones, or UAVs, are a low-cost alternative to missiles and air-dropped bombs. The Shahed 136 'kamikaze'-type drone carries a 40-kilogram payload and can fly up to 2,400 kilometres at around 100 kilometres per hour. It is designed for a one-way mission, crashing into its target, and effectively functioning like a cheap missile. Intelligence or information-collecting UAVs (or surveillance drones) are relatively small, navigated drones which may or may not carry explosive payloads. Some surveillance drones can be used to coordinate ballistic missile attacks. The presence of such drones can serve as a warning indicator.

Direct targeting of humanitarian actors, though possible, is less likely than the risk of collateral damage. The weapons used will have different approach times and some may be easier to intercept than others. Ukraine developed a country-wide app-based notification system in 2022 to provide air raid warnings with information about the type of incoming weapon. Organisational protocols can be put in place that direct staff to take shelter underground or in an interior room, depending on the type of strike.

Shelling/artillery fire from land-based platforms

Shelling from land-based platforms typically targets an opposition force's positions (such as bunkers and trenches) and movements. It is often used to disrupt supply lines, depots and logistics hubs. Basic distinctions can be made between random or saturation fire, predicted fire and observed fire.

- Random or saturation fire is highly inaccurate. It can be the result of the type of weapon used, such as multiple rocket launchers, which saturate an area with shells, or a deliberate tactic, such as an artillery barrage or so-called carpet-bombing.
- Predicted fire is less random. Aiming relies on map-based calculations, with no capacity to adjust to a specific target.
- Observed artillery fire or air attack means that drones or human observers on the ground watch where shells, rockets or bombs are landing, and relay directions to guide targeting for the firing crew. This type of fire can be very accurate and allows for following or switching targets.

Anti-armour weapons and RPGs are shoulder-fired weapons that launch rockets with explosive warheads. They are commonly used against armoured vehicles, fortifications and enemy personnel in direct line-of-sight. They are portable, versatile and easy to use. Avoidance – that is, remaining outside of their 200–500-metre range – is the best mitigation. If inside that range, minimising time spent in open areas and avoiding predictable patterns of movement can reduce the risk of being targeted, and armoured vehicles and fortified shelters can be critical mitigation measures.

Crossfire and sniper fire

Crossfire is a risk in the proximity of any small arms or artillery fire. Although most small arms fire is usually effective only up to 300 metres, some machine guns have an effective range of over 1,800 metres and bullets can travel up to 6 kilometres. Sniper fire is targeted, and certain sniper rifles can strike a target from a long distance (over 1 kilometre).

The best defence against crossfire and snipers is to reduce exposure by keeping staff out of range (which may be possible only when battle lines are relatively stable), and away from areas where small arms fire is being exchanged or snipers are operating. In sudden crossfire, when staff are not the target, they should get on the ground immediately and try to move to a safer place. When inside, they should stay away from windows and doorways and try to get at least two

walls between themselves and the bullets. This will also increase protection from ricocheting bullets.

These precautions also apply in the event of 'celebratory fire' such as can occur at parties or demonstrations, where injuries and fatalities from falling bullets are a serious risk.

Active shooter prevention and response

Active shooter incidents are a critical threat in certain contexts, with the potential for mass casualties and significant psychological impact on survivors. Humanitarian organisations are not immune to such threats, which can occur with little or no warning. Risk mitigation usually requires multiple layers of security, each designed to slow or block the shooter's access to buildings or compounds. The innermost layer is typically a reinforced room.

Understanding the indicators of potential violence, implementing mitigation measures and having a well-rehearsed response plan can significantly reduce the risks associated with active shooter events. Training may include guidance on a 'run, hide, tell' strategy.

- **Run.** If there is a safe path, attempt to evacuate the area. Encourage others to leave with you, but do not let their indecision slow you down. Leave your belongings behind and keep your hands visible to armed responders.
- **Hide.** If evacuation is not possible, find a place to hide. This should be out of the shooter's view, provide protection if shots are fired in your direction and, if possible, not restrict options for exit. Lock and/or barricade the doors, turn off lights and silence any phones. If an active shooter event is likely, construction of a reinforced safe room should be considered.
- **Tell.** Once safe to do so, emergency services (or other emergency contacts per organisational protocol) should be called and provided with as much information as possible. This includes the location of the shooter, a description of the shooter and their weapons, and the number of people at the location.

Mines, improvised explosive devices and unexploded ordnance

Mines

Armed groups lay mines to defend their positions, disrupt enemy movements, deny the enemy access to certain routes and/or channel the enemy onto a certain route. They can also be placed around potential targets such as power pylons (transmission towers), water and electricity plants and rail junctions, to protect against sabotage and attack. Mines have been used in civilian and agricultural areas to cause general fear and dislocation. Once laid, mines can move a considerable distance as a result of flooding or landslides.

There are generally two categories: anti-tank mines and anti-personnel mines.

- **Anti-tank mines** are large and have substantial explosive power. They typically require a heavy weight or movement to activate, but this may not be the case if they are old and unstable, and they can cause almost total destruction to a non-armoured vehicle (including most civilian armoured vehicles, which are only protected against small arms).
- **Anti-personnel mines** are smaller. Some are designed to cause injury by removing a hand or foot. Others can do much more serious, even lethal, damage. Direct fragmentation devices are designed to scatter ball fragments to kill or wound up to 500 metres in a particular direction.

Case example: repeated mining

In 1995 an NGO vehicle hit an anti-tank mine on a road in Central Africa. The explosion killed two passengers and injured three others. During the night, new anti-personnel mines were planted around the wreckage. The next day, a local woman who had come to look stepped on one and lost her leg.

Mine awareness training for staff is an essential element of security risk management in areas where mines are being actively used or remain from previous conflicts. This includes:

- Staying vigilant and knowing what to look out for.
- Mine and UXO identification, marking and reporting.
- Avoidance techniques.
- What to do when in a mined area in a vehicle or on foot.
- Emergency response (in case of detonation and injury).

International specialist humanitarian demining organisations such as the HALO Trust and the Mines Advisory Group provide training and information. In the country itself, the main sources of general and locality-specific information include:

- The national mine action organisation or the local authorities and security forces.
- Demining organisations, and a central UN mine action centre.
- UN military observers or peacekeepers.
- Hospitals and health posts dealing with mine casualties.
- Local people.

Local knowledge is especially important. When venturing into a new area where there is active fighting or there has been fighting in the past, organisations can inquire about the history of fighting in the area; accidents – have vehicles, people or animals been hit by mines, and if so when and where?; where local people go and what areas they avoid; which roads or sections of roads have been used and to what extent; and how roads are used – do locals walk, use bicycles or vehicles? Anti-tank mines may not have been detonated and will remain a danger.

Local people often create their own warning signs to mark minefields – but these can be hard for outsiders to identify and can be ambiguous or unclear. Signs may be nothing more than a small heap of pebbles or two crossed branches lying at the start of a path. Local people can be asked what signs they use, and whether they have a common system – if everybody does it their own way, there is no common signal. Demining operations mark identified fields in different ways in different countries but usually the signs are clear enough. The colour red is normally used in markings. It is important to remember that signs may have fallen down or become obscured.

Improvised explosive devices

IEDs can be used to target military vehicles, sites or personnel, as well as civilians. They are also commonly used to deny access to areas or routes. They can be detonated by remote control, time-delayed or triggered by the victim. Devices commonly triggered by the victim, such as stepping on a pressure plate or pulling a trip wire, require cautious movement restrictions. Time-delayed devices typically target a pattern of activity or are delayed in order to allow the perpetrator to escape. Remote-controlled or command detonation devices can be more exact. Often IEDs are planted by a retreating force to complicate the reoccupation of an area. When used as booby traps, they are hidden or disguised: a door or window of a house can be booby trapped, as can a well, a dead body or an innocent-looking household item like a toy. A common tactic involves striking a target, then hitting the same location soon afterwards to target rescuers and bystanders who arrive to help the injured. It is important to understand how IEDs are being used so that the organisation can adjust its SOPs accordingly.

Unexploded ordnance

UXO refers to material that was intended to explode on impact but failed to do so. Artillery and mortar shells, and even small arms ammunition, can remain explosive and become increasingly unstable over time. Bombs and shells may have buried themselves deep in the ground, presenting a continuing danger, for instance to farmers and builders. Destroyed or abandoned military or militarised vehicles and buildings used by armed groups may contain UXO, as well as volatile fuels and chemical residues. UXO may pose a much greater threat than landmines because their dispersion may be more random and unpredictable, and because the munitions themselves are likely to be unstable. A particular risk are cluster munitions delivered by artillery shells or from a plane. In mid-air, the containers break up and then distribute a multitude of bomblets that can saturate a whole area.

Essential guidance for staff – mines and UXOs

When dealing with mines and UXOs, advice to staff should be: do not touch, do not approach, mark if possible, report.

UXOs are generally visible, although they can be partly or even wholly buried. They should be presumed unstable and not touched. Staff should mark their position and inform the authorities.

Any object large enough can be improvised/booby-trapped to carry explosives. The object that is booby-trapped is generally visible – but not the explosive linked to it. Anything in an uncleared area can potentially be booby-trapped, so staff in the area should not enter empty buildings or ruins, and should not pick anything up or open shutters or doors.

Mines are generally not visible. In an area where mines have been used, staff should not travel on any road that has not been confirmed cleared. If a mine is seen, the location should be marked and the authorities informed.

Untrained people should never handle mines and UXOs. A standard HEAT course does not count as training in this regard.

Chemical, biological, radiological and nuclear threats

To date, humanitarian organisations have had little direct experience of CBRN threats. In reality, no humanitarian organisation is currently equipped to protect its staff – much less local civilians – in the event of a catastrophic CBRN event. Most of the organisations that have taken the decision to operate in major conflict zones have decided that the likelihood of an occurrence is low enough to accept the risk. However, the risk is never absent in any major conflict setting, so it is important to assess and discuss the risk, and consider mitigation measures.

Chemical weapons were deployed several times in the Syrian civil war (starting in 2012) and in Ukraine (starting in 2022), where the additional risk of deliberate or accidental nuclear events was frequently discussed among humanitarian organisations operating there. Risks can include the following:

- Industrial accidents, such as a fire or explosion at a chemical plant or storage facility, an accident at a nuclear power plant or a leak from a biological containment facility. Such incidents can release toxic substances into the environment, posing immediate and long-term health risks to the population and responders.
- Accidents during transport of CBRN agents for industrial or military purposes.
- Hazards like earthquakes or tsunamis can damage industrial plants or military storage facilities, potentially leading to the release of CBRN materials.

- Collateral damage to industrial plants, hospitals (radiology departments) or research, manufacturing and military facilities as a result of conflict.
- Direct attacks by armed forces releasing chemical or biological agents to cause mass casualties or other groups using CBRN materials to create weapons such as 'dirty bombs' (radioactive dispersal devices).

Individuals can be exposed to CBRN hazards in various ways, including inhalation, physical contact (between people or with objects) and consumption of contaminated food or water.

For risk mitigation purposes, key questions to consider include who the most at-risk staff would be (such as medical personnel), whether there are expert-informed SOPs that can be adopted (such as the use and nature of PPE), what contingency plans can be put in place (such as withdrawal, evacuation and emergency medical support) and whether specialist training is advisable for the most at-risk staff, such as how to reduce exposure if contamination is suspected. Any security risk management measures must be informed by specialists.

White phosphorous

White phosphorus is used in a combat zone to provide a smokescreen. It clouds very quickly, not only obstructing visual contact but also scrambling infrared radiation, thereby interfering with infrared optics and weapon-tracking systems, such as those used by guided weapons like anti-tank missiles. It can be delivered by small smoke grenades, tank cannons and mortars or other artillery. On explosion, burning particles spray outward, followed closely by streamers of white smoke, which then coalesce into a very white cloud.

While its stated use may not be as a 'chemical weapon', white phosphorous is nonetheless a toxic chemical that, when used in populated areas, has harmful effects on people. The burning particles stick to skin and can produce serious burns. Particles continue burning until completely consumed or until they are deprived of oxygen. In addition, phosphorus can be absorbed into the body through the burned areas and cause liver, kidney and heart damage or even organ failure. Phosphorus particles can also be orally ingested. Inhalation of the smoke is hazardous and will irritate the eyes, nose and respiratory tract, but does not pose the same lethal threat as burns and ingestion.

Further information

General research

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).

Armed conflict risk mitigation

ICRC (2006) *Staying alive: safety and security guidelines for humanitarian volunteers in conflict areas* (https://reliefweb.int/report/world/staying-alive-safety-and-security-guidelines-humanitarian-volunteers-conflict-areas).

ICRC (2021) *SAFE: security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Torelli, C. (2024) *Explosive violence monitor 2023*. Action on Armed Violence (https://aoav.org.uk/2024/explosive-violence-monitor-2023/).

Wilson, O. (2017) *Counter-terrorism: IED, bomb, and active shooter procedures.* Risks Incorporated (https://gisf.ngo/resource/risks-counter-terrorism-procedures/).

Chemical, biological, radiological and nuclear threats

European Union CBRN Risk Mitigation Centres of Excellence Initiative (n.d.) *Chemical, biological, radiological and nuclear risk mitigation* (https://cbrn-risk-mitigation.network.europa.eu/index_en).

ICRC (2014) *Chemical, biological, radiological and nuclear response: introductory guidance. For training purposes only* (www.icrc.org/en/doc/assets/files/publications/icrc-002-4175.pdf).

IFRC (2023) *Chemical, biological, radiological and nuclear (CBRN) hazards* (https://epidemics.ifrc.org/manager/disaster/chemical-biological-radiological-and-nuclear-cbrn-hazards).

Roper, R. and Goodzey, C. (2005) 'Extreme emergencies: humanitarian assistance to civilian populations following chemical, biological, radiological, nuclear and explosive incidents – a sourcebook' *Journal of Homeland Security and Emergency Management* 2(2) (https://doi.org/10.2202/1547-7355.1146).

UN (2019) 'Policy on chemical, biological, radioactive and nuclear threats and attacks' *Security management*, Section Q, Chapter 4 (https://policy.un.org/en/security/specific-security-considerations/chemical-biological-radiological-and-nuclear-threats-and).

Mines and unexploded ordnance

United Nations Mine Action Service (UNMAS) (2015) *Landmines, explosive remnants of war and IED safety handbook* (www.unmas.org/en/landmines-erw-and-ied-safety-handbook).

UNMAS (2023) *Marking explosive ordnance hazards*. IMAS 08.40 third edition (www.mineactionstandards.org/standards/08-40/#:~:text=The%20marking%20of%20explosive%20ordnance,unintentional%20entry%20into%20hazardous%20areas).

Personal protective equipment

National Institute of Justice (2024) *Understanding NIJ 0101.06 armor protection levels* (https://nij.ojp.gov/library/publications/understanding-nij-010106-armor-protection-levels).

Afterword

Humanitarian security risk management has made significant progress over the past two decades, shifting from a largely reactive stance to a proactive approach more aligned with aid organisations' strategic and operational goals. This progress has enabled humanitarian action to continue in increasingly dangerous environments, supported by better-trained staff, more sophisticated security systems, improved interagency coordination and a growing focus on personal risk profiles and staff wellbeing. Despite this, notable gaps remain.

There continues to be significant disparity between organisations in terms of resources, with local organisations still often lacking the necessary funding, tools and training to manage risks to the same degree as their international counterparts. Secure access in conflict areas – especially in conflicts involving large state actors – remains restricted. Additionally, digital security risks, increasingly fragmented conflict environments and the challenges of climate change have added further layers of complexity to humanitarian operations, which most existing security risk management systems are not yet equipped to effectively address.

Looking forward, the sector needs to ensure local aid workers and organisations are not left behind in the development of security practice. Equitable partnerships, two-way knowledge transfer and increased direct funding can support this. AI and digital tools are improving threat detection, risk assessment and coordination, but they also introduce new challenges, risks and threats. Future security risk management systems will need to incorporate these technologies effectively while remaining vigilant about the risks.

A person-centred approach to security needs to be more widely adopted, recognising the diverse risk profiles of aid workers – their strengths and vulnerabilities – and tailoring security risk management practices to meet individual needs. Security risk management must also become more forward-looking, adaptive and agile to match the pace of change in global threats and effectively respond to new risks as they emerge. Although this GPR presents a wide and detailed array of practices and tools for security risk management, these must align with the needs and capabilities of organisations and their staff. The system should serve the people, not the other way around.

Finally, increasing violence against aid workers, particularly by state actors, underscores the need for stronger accountability. UN Security Council Resolutions emphasise this, and greater collaboration between security and advocacy teams within organisations can support efforts to strengthen accountability measures to better protect humanitarian actors.

Adelicia Fairbanks
Lead Editor