eisf

AN EISF GUIDE FOR NON-GOVERNMENTAL ORGANISATIONS

Security Risk Management:

a basic guide for smaller NGOs

EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent over 80 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Federal Department of Foreign Affairs (FDFA), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Acknowledgements

This guide was developed by Shaun Bickley (Tricky Locations) with input from Lisa Reilly (EISF Executive Director). The project manager and editor was Adelicia Fairbanks, Research Advisor at EISF.

The author and EISF would like to thank the following people who contributed their time and expertise to the development of this guide: Gonzalo de Palacios, Marta Iglesias (MPDL), Nathanael Jarret, Andrew Parkes (Malaria Consortium), Laky Pissalidis, Emmanuelle Strub and Lotta Westerberg.

Suggested citation

Bickley, S. (2017) *Security Risk Management: a basic guide for smaller NGOs*. European Interagency Security Forum (EISF).

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

Design and artwork : www.wave.coop

Contents

Introduction

The security of personnel is one of the biggest challenges facing humanitarian and development non-governmental organisations (NGOs), large and small, as they are faced with growing insecurity, threats and violence.

While working and travelling in such unpredictable environments will always carry a degree of risk, organisations can do much to develop a safer and more secure working environment for their staff. However, this requires increased prioritisation and resourcing of security risk management by the organisation. For many NGOs, security risk assessments, security plans, travel security procedures, security training, and incident reporting systems are now a key part of their operating language and are central to how they work around the world.

To a smaller NGO, however, such mechanisms may seem excessive or too costly to implement, given the size of the organisation, the environments in which staff work, and the activities they undertake. Regardless of size, however, all NGOs have a duty of care obligation towards their personnel. Staff from smaller organisations often find themselves working in the same areas and exposed to similar threats with very little support when compared to their counterparts from larger organisations with significant security architecture in place. Many staff find the lack of priority and support given to security, or the disparity between how organisations approach security, frustrating and stressful, and often feel that their organisation is placing them at increased risk. Therefore, it is vital that an effective framework is established that embeds security risk management practices across your organisation.

Even when organisations recognise the need to improve their approach to staff security, it can still seem a daunting task. Where do you start? What are the priorities? Who will undertake the work? Often the individuals given this responsibility have limited security risk management experience and training and are juggling other priorities and roles. While not without its challenges, enhancing staff security must be a core priority for NGOs of all sizes. Organisations that manage risks effectively will have greater access to, and ultimately more programme impact in, insecure environments, while also safeguarding their staff.

'Security' vs 'safety'

The terms 'security' and 'safety' are often used interchangeably, but they do have different definitions. Security is primarily concerned with intentional acts of violence, aggression and/or criminal acts against agency staff, assets or property, whereas safety relates to unintentional or accidental acts, events or hazards.

There are many overlaps in the measures required to manage both security and safety risks, and sometimes critical safety incidents, such as vehicle accidents, can have additional security implications. While some organisations make a clear distinction between the two and even have separate security and safety management structures, most smaller organisations will use the same resources to manage both security and safety issues. Therefore, for the purpose of this guide 'safety' is also implied whenever reference is made to 'security'.

About this guide

This guide aims to be a simple, easy-to-use security resource to help smaller NGOs demystify security risk management. By setting out the elements of a basic security risk management framework, this guide aims to support NGOs in translating their duty of care obligations into key processes and actions that will not only enhance their national and international staff security but also improve their organisation's reputation and credibility. Although the guide is intended to be applicable to both national and international NGOs, some elements may be more relevant to one or the other.

Many existing NGO security resources tend to focus on the requirements of larger humanitarian and development organisations, i.e. those with large multi-national staff teams working in multiple countries, often with dedicated security staff. This guide is mindful of the limited resources and the specific challenges that smaller NGOs may face in trying to establish and maintain a security risk management framework.

This guide complements other essential guides, such as EISF's 'Security to go', which focuses on security management systems in a particular context or location; however, this guide provides a broader perspective on the overarching framework an organisation should aim to have in place in order to improve its security risk management. This guide also aims to complement the EISF 'Security Audits' guide, which enables organisations to take stock of what they have in terms of staff security and what needs to be improved.

Who is this guide for?

This guide is aimed principally at staff within smaller NGOs who have a level of responsibility for the security of staff and are looking to enhance security risk management within their organisations.

Although written specifically with smaller NGOs in mind, the guide is relevant to organisations of any size, even large and well-established organisations whose staff travel to and work in challenging environments. This guide can also be useful for international NGOs that do not have in-country presence but rather are seconding their staff into partner organisations.

How to use this guide

The guide is structured around the key building blocks of a security risk management framework. Readers can easily navigate and consult specific aspects of the framework depending on the area of security risk management that they are looking to address. Throughout the text are:

- Crucial activities and tips, indicated with 🔔
- Expert accounts, indicated with 💬
- Cross-references within the guide, indicated with ▶
- Cross-references to further security resources, tools and supporting information, including EISF publications which are available at www.eisf.eu, indicated with 📖
- Hyperlinks are provided for easy navigation.
- Please refer to the bibliography for details on, and links to, resources cited in the text.

1 Fulfilling duty of care

Although most NGOs, large and small, recognise that they have a responsibility to protect their staff, many organisations still fail to appreciate the full extent of their duty of care obligations and the implications that these have for security risk management. The duty of care benchmark has risen significantly over the past decade, and what was once considered good enough would certainly not be considered adequate today. Although duty of care is a legal term for the responsibilities organisations have towards their staff, there is also a moral obligation of duty of care that organisations should consider.

Essentially, duty of care means ensuring that appropriate mitigation measures and support are in place to prevent and respond to incidents and that all staff are adequately informed of the risks and the corresponding mitigating measures.

It is important to stress that duty of care is more than just security. Security risk management is just one element in an organisation's overarching responsibility for the health, safety, security and wellbeing of its staff.

Duty of care obligations are not restricted to contractual relations such as those between employer and employee. Organisations also have a duty of care towards those who are acting on behalf of the organisation, such as independent contractors, consultants, volunteers, dependants and official visitors.

Often, the level of responsibility an organisation has towards an individual is determined by the extent to which that person has control over their work environment and the tasks they undertake, and their access to information about prospective risks; the higher the degree of control or influence an organisation has, the greater its responsibility. For example, when an NGO arranges a visit from a consultant, including planning itineraries, travel arrangements, securing accommodation and transportation, it becomes more responsible for the security of that consultant. This is especially true where the organisation, through its presence or activities in the country, is in a better position than the visitor to monitor the risks.

Often, smaller NGOs will not have fixed offices in the country, but staff will travel individually and/or be embedded within a partner organisation. The employing organisation still retains the legal duty of care responsibilities and must ensure that the security risk management of the partner organisation is appropriate to meet these responsibilities.

Your duty of care

All organisations have a legal and moral obligation to provide a standard of care to safeguard employees, and those acting on behalf of the organisation, from a reasonably foreseeable risk of harm. To meet your basic duty of care, you must:

- **Know the risks** – organisations must be able to demonstrate that they have identified and considered all foreseeable risks related to a particular location or activity. Risk assessments must be regularly updated and documented.
- **Establish mitigation measures** – organisations must take all reasonable measures to manage risks. Comprehensive, up-to-date plans, procedures and mechanisms must be in place and adhered to in order to address the risks that exist in a particular location or associated with a specific activity. Adhering to local community standards allows you to demonstrate that you are aware of what is considered common good practice among other NGOs in the area you are working in.
- **Develop emergency plans** – detailed plans, measures and assistance must be in place to respond to emergency situations involving staff, regardless of the location.
- **Ensure informed consent** – staff must understand and accept the risks they face and the measures in place to manage them. There must be a process in place to document their understanding of the risks and their role in managing them. However, such documents will not provide a legal waiver in a court of law.
- **Raise awareness** – staff must receive detailed, up-to-date information and guidance, and in many cases training, related to the risks that they are exposed to.
- **Provide appropriate support** – organisations must have appropriate support and insurance in place to assist staff affected by an incident.

Duty of care responsibilities apply equally in both high- and low- risk environments. However, it is expected that organisations take even greater responsibility for staff working in higher risk situations. It is recognised that not all risks can be removed, particularly in high-risk environments. Therefore, a lot of weight is placed upon the 'reasonableness' of actions, and on staff being provided with the information needed to make an informed decision about the residual risks they could still be exposed to.

Further information

EISF article 'Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications' by Edward Kemp and Maarten Merkelbach

EISF guide 'Security Audits'

'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff' by Edward Kemp and Maarten Merkelbach

'Voluntary Guidelines on Duty of Care to Seconded Civilian Personnel' by Maarten Merkelbach

Defining risk attitudes

NGOs have very different levels of exposure and attitudes to risk depending on their mandate and values, the perceived need for or benefits of their activities, and ultimately their capacity to absorb or manage the risks to which their staff are exposed.

Be risk aware rather than risk averse.

It is vital that all organisations identify their unique risk profile and determine the level of risk they are willing to accept. The risks that confront staff should always remain proportionate to the need or benefits of specific activities, the organisation's ability to manage these risks, and the consequences if something were to happen. Providing staff with a benchmark as to your organisation's risk attitude, sometimes described as a 'risk threshold', will help guide decisions, for example, on whether to authorise visits or begin activities in certain locations with a higher level of risk, or when to stop or suspend activities or withdraw staff due to deteriorating security or specific threats.

All staff must have a shared understanding of the level of risk their organisation is willing to take for specific activities, and when and how to escalate decisions up the management line. Key organisational security documents, such as your NGO's security policy, should include a clear statement on the organisation's attitude to risk, together with information on how these risk thresholds are assessed, and the authorisation processes and security measures required in relation to different levels of risk.

▶ *See section 6: Travel management and support*

Further information

EISF briefing paper 'Risk Thresholds in Humanitarian Assistance'

'Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management' by Oliver Behn and Madeleine Kingston

ISO 31000:2009

Establishing a security culture

A positive security culture is key to enhancing your organisation's staff security. The 'culture' of an organisation can be simply defined as 'the way we do things around here'. Every organisation has a cultural attitude towards security and risks in general. The difference is that some organisations encourage secure working, while others do not. It is not enough for an organisation simply to state that it takes security seriously and has policies and procedures in place if the organisation's culture does not engender a positive approach to security. All staff within the organisation need to understand and demonstrate the organisation's values in how they go about their activities on a day-to-day basis.

'Where organisations have no embedded security culture, the culture in each location is dependent on the individuals in that location; meaning multiple different security and safety approaches across the organisation, some of which are good and some of which are not good enough – with the overall result being that the organisation does not have its own security culture – something which staff quickly recognise and hold against the organisation.'

NGO Security Advisor

Creating a positive security culture in your organisation will require a collective sense of awareness and responsibility among all staff; where each and every staff member, including those in senior leadership, takes personal responsibility for their security and actively ensures that it is integrated into all aspects of programmes and activities. Simple actions such as an annual award for compliance or including drivers in security planning, for example, can have a noticeable impact on attitude and behaviour without needing significant additional resources.

A positive security culture cannot be created overnight: it takes time to change staff attitudes and behaviours, and thus the organisation's overall approach, to security risk management. You will certainly face barriers and difficulties, and some level of internal resistance, non-compliance and resource limitations. It is important to be realistic, recognise that establishing a positive security culture is a long-term process, and plan accordingly. It is better to start with easily achievable targets, which will help create a momentum for 'cultural change', and build up from there. A partial security risk management system is certainly better than no system being in place at all.

'We had all the security policies and procedures in place, but the organisational culture did not change until the CEO took the personal security course.'

INGO Humanitarian Manager

Further information

'Developing a Security-Awareness Culture – Improving Security Decision Making' by Chris Garrett

11 steps to a positive security culture

1. **Develop a framework** – outline the organisation's approach to security, including the policies, procedures and mechanisms which have been put in place to ensure effective security risk management.
2. **Draft a policy** – outline the organisation's risk attitude and key security principles, and define roles and responsibilities. Include security responsibilities and obligations in the job descriptions of all staff members and senior managers.
3. **Raise awareness** – engage all staff to ensure everyone is aware of and in agreement with the priorities for improving security risk management from the Board down. Ensure senior management issue clear statements on the importance of staff security. Measures should be 'owned' by staff and not perceived as having been imposed from the top of the organisation without staff consultation or agreement.
4. **Lead from the front** – ensure that any security practices, such as personal security training or trip planning forms, are mandatory for all from the CEO down.
5. **Provide flexible options** – security risk management is not a 'one size fits all' approach. Ensure locally relevant measures and plans are established in different security contexts and risk environments.
6. **Look for 'quick wins'** – identify measures or requirements which can be established quickly, with limited time and resources, but which can have a positive effect on staff security.
7. **Report, report, report** – stress to staff the importance of reporting incidents and near misses, and of sharing their security concerns. Ensure that there are easy and effective mechanisms in place to report and capture incidents.
8. **Establish security forums** – ensure that various meetings or mechanisms exist within the organisation where security issues and challenges can be raised and discussed. Ensure security is a standing agenda item at key meetings.
9. **Monitor and review** – undertake periodic reviews of the organisation's security approach and management framework, and their implementation, to ensure the framework remains effective.
10. **Enforce accountability** – establish a mechanism to hold people accountable for security, and ensure security risk management responsibilities are included in staff performance reviews.
11. **Celebrate success** – identify positive approaches and find champions to help motivate others on the positive impacts of improved security: better security, better access, better outcomes.

Resourcing security risk management

There are inevitable costs associated with managing security. Developing and rolling out a comprehensive approach to security risk management can take significant time and financial resources – both limited commodities in all organisations.

For smaller NGOs, limited capacity and funding are often perceived as the major barriers to addressing security effectively. However, there are many aspects of security risk management that do not require significant time or large security budgets for them to be addressed. For example, numerous 'open source' risk management templates, tools and resources are available (through, for example, EISF and InterAction) and can be easily adapted and used by NGOs. In addition, while security training can be a major investment for smaller organisations, there are many freely available online courses that can assist in raising the security awareness and capacity of staff.

▶ *See section 7: Awareness and capacity building*

There is also a growing acceptance by donors that staff security is an essential element of programming in insecure areas. Many major donors are willing to fund some security costs. For example, conducting security assessments and audits, establishing security positions, purchasing essential security-related equipment, improving the security of key facilities, and providing training are all costs that many donors are now willing to fund. It is key for NGOs to identify and justify security costs through a risk assessment, and ensure that security considerations and costs are incorporated within programme proposals and budgets, and not just included as part of overhead (i.e. indirect) costs.

📖 *See EISF briefing paper 'The Cost of Security Risk Management for NGOs'*

While there will be many 'easy wins' for your organisation as it improves its approach to staff security, ultimately it is a question of prioritisation and resources. Building an effective security risk management framework will require the commitment of sufficient financial and human resources; it is important that this is discussed early on and a commitment is sought from senior management level to prioritise and resource security appropriately.

Further information

EISF briefing paper 'The Cost of Security Risk Management for NGOs'

'The Risk Management Expense Portfolio (RMEP) Tool' in 'The Cost of Security Risk Management for NGOs' briefing paper

2 Developing a framework

The first step in establishing an effective system to safeguard staff is to develop a security risk management framework that explains the architecture, roles, responsibilities and arrangements in place to support better access through improved staff safety and security.

A Security Risk Management Framework is a set of policies, protocols, plans, mechanisms and responsibilities that supports the reduction of security risks to staff.

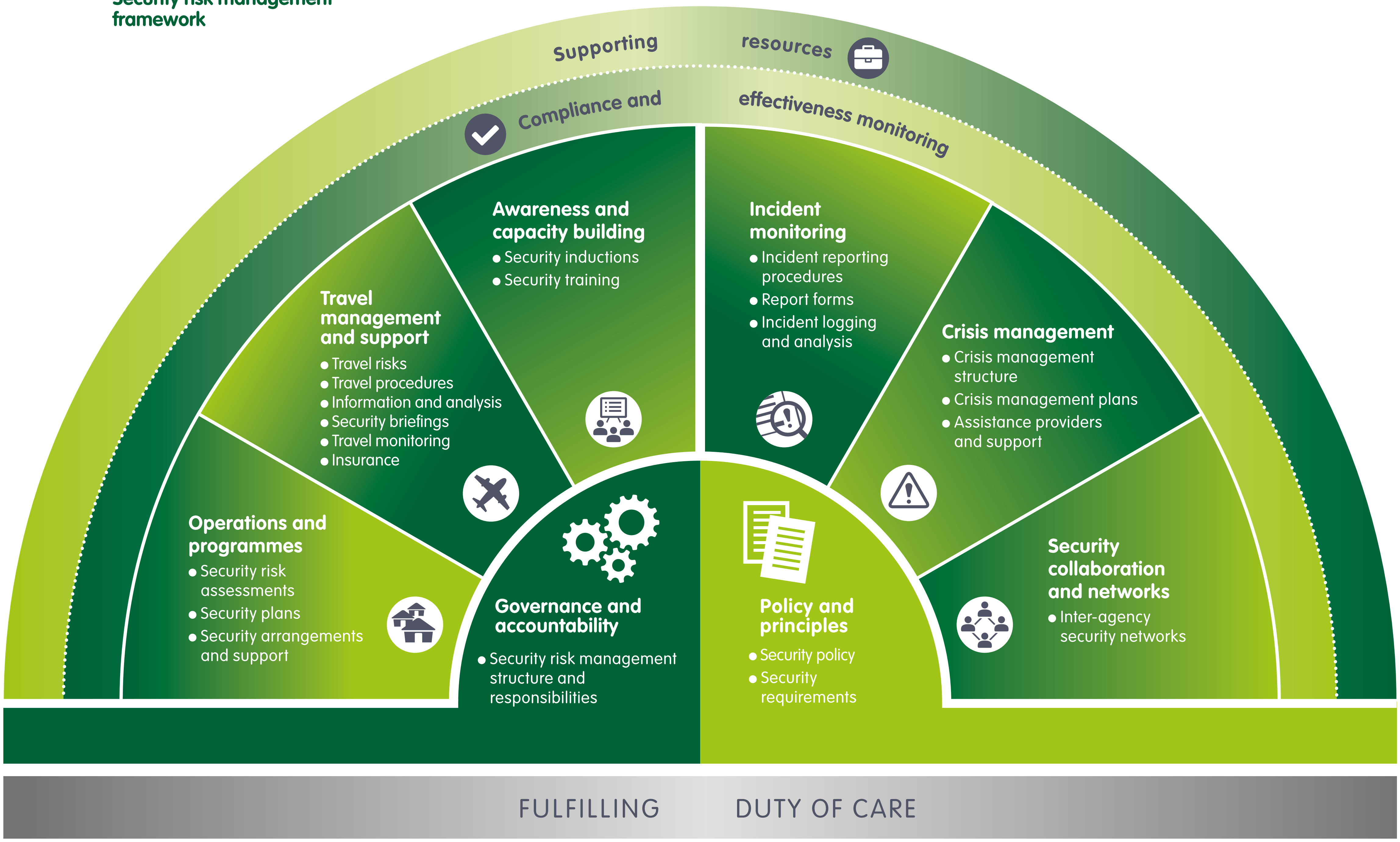
Your organisation needs to manage a wide range of risks including financial, operational, legal, and reputational risk. Security risk management is only one element in the organisation's overall management of risk and must be aligned with the organisation's wider approach to risk management together with existing policies and processes. A basic security risk management (SRM) framework is one integrated system with two main elements:

- The **foundations**, which include good security governance and an accountable structure, as well as a security policy and principles.
- The **mechanisms**, which include the various security procedures, plans, activities and supporting resources used to manage security risks to staff.

To be clear – the security risk management framework is NOT a single document. However, you will need to develop an outline document or 'map' that explains how the framework delivers your organisation's approach to security risk management, and how all the various documents and processes that form part of the security risk management framework relate to each other.

The diagram overleaf illustrates the essential building blocks of a security risk management framework and how they fit together.

Security risk management framework



Supporting resources

Compliance and effectiveness monitoring

Operations and programmes
- Security risk assessments
- Security plans
- Security arrangements and support

Travel management and support
- Travel risks
- Travel procedures
- Information and analysis
- Security briefings
- Travel monitoring
- Insurance

Awareness and capacity building
- Security inductions
- Security training

Incident monitoring
- Incident reporting procedures
- Report forms
- Incident logging and analysis

Crisis management
- Crisis management structure
- Crisis management plans
- Assistance providers and support

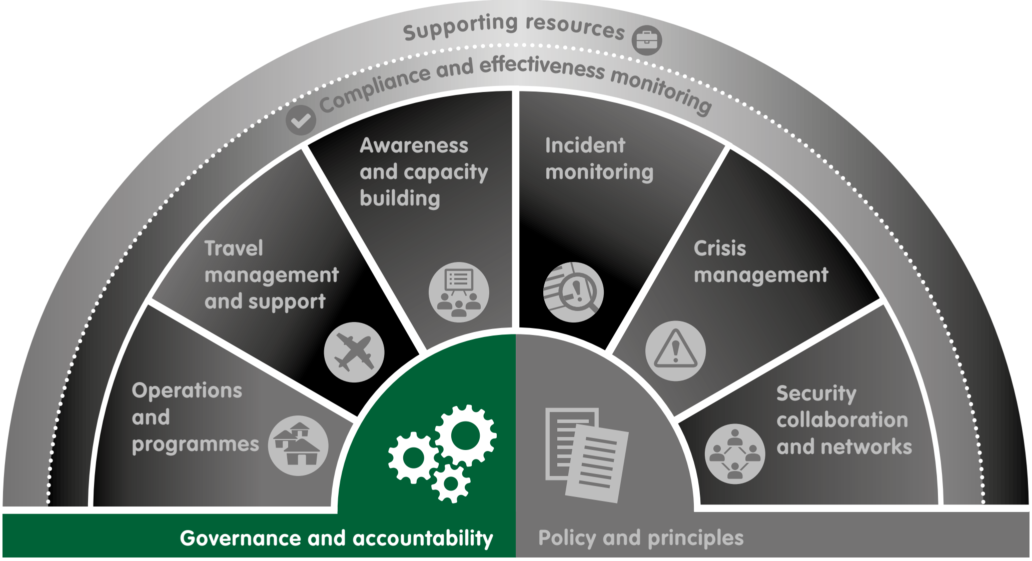
Security collaboration and networks
- Inter-agency security networks

Governance and accountability
- Security risk management structure and responsibilities

Policy and principles
- Security policy
- Security requirements

FULFILLING DUTY OF CARE

3 Governance and accountability


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Good governance and accountable structures are the backbone of any effective security risk management framework. Staff at all levels within an organisation – from the Board of Trustees to the individual staff member – have a collective responsibility to manage and reduce risks to staff. While individual employees must bear a degree of responsibility for their own security, all organisations, regardless of size, must ensure that an effective management structure is in place that fosters a positive security culture and helps the organisation fulfil its duty of care obligations.

Creating an effective security risk management structure

Ultimate accountability for staff security and safety will rest with the Board of Trustees who then delegate responsibility to the Executive Director/CEO, or a position of similar seniority, to ensure that effective security risk management is in place. Day-to-day management and responsibility for security is then shared across different levels in the organisation and usually follows a management line model. All staff with security responsibilities must have their duties clearly articulated in their job description, and, for accountability, assessed in their performance reviews.

Choosing the right people to lead on security is the key to success. Many larger organisations now have dedicated security advisors, or even security teams, to oversee the organisation's security framework and to provide security support and advice. For smaller NGOs, however, this model is unrealistic.

Identify someone or even a group of staff within your organisation who can act as a focal point for security and lead on developing and implementing the security framework. It is important that these people are given adequate time, support and training to do this in addition to their usual tasks.

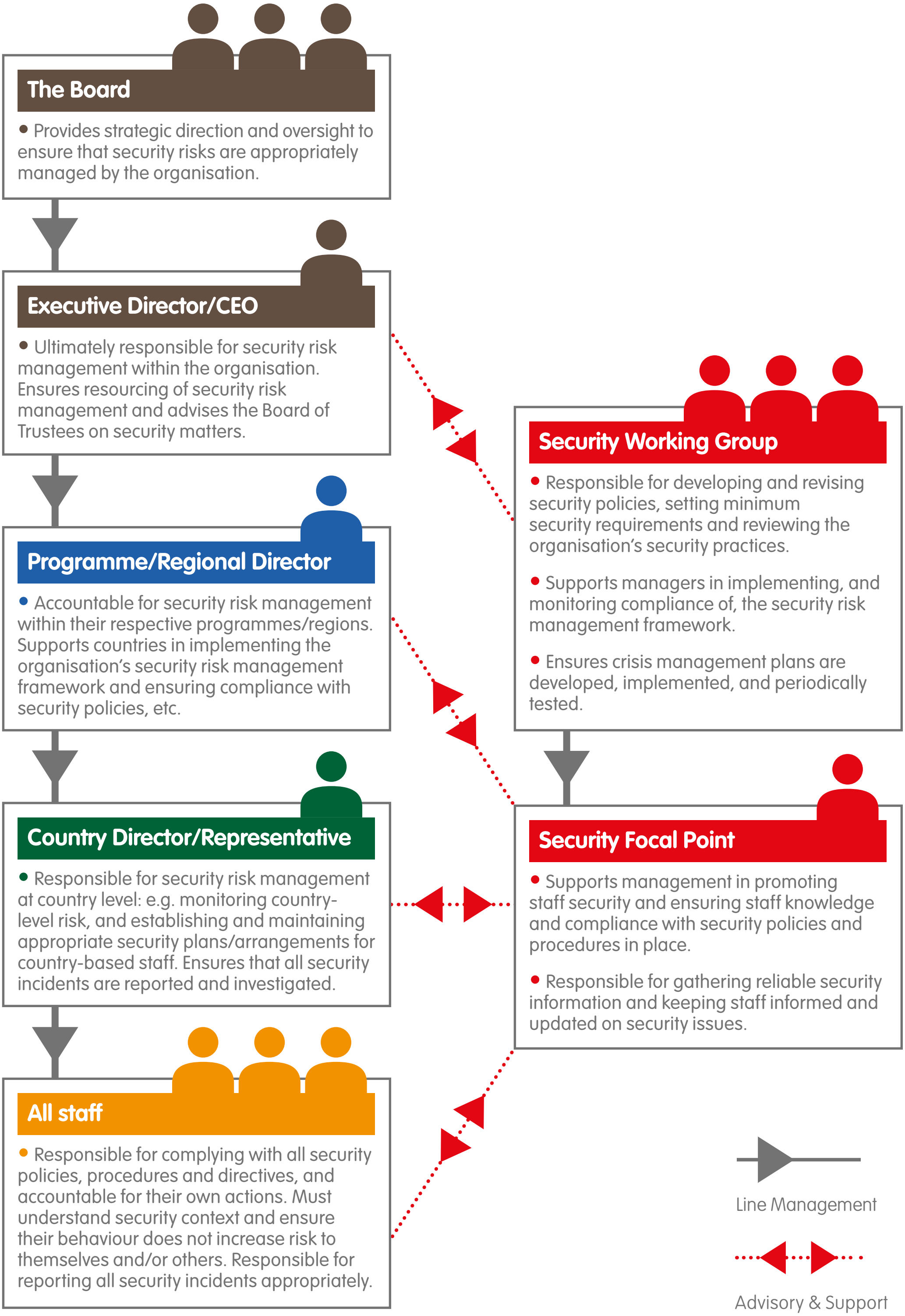
Managing risks to staff is a shared responsibility. Embedding good security risk management requires clearly defined roles and responsibilities, and structures that have sufficient capacity to provide and maintain effective support.

Many organisations use a security working group or committee of representatives of different roles and levels within the organisation. This collective approach helps share the load, brings a wide range of experiences and perspectives, and encourages a greater sense of ownership which ultimately aids implementation and compliance.

It is important to note that the security focal point or working group is not responsible for managing security risks (that is to say, they do not 'own' the risk). Instead, security management responsibilities must remain embedded within normal programme management. The role of the security focal point or working group is to support the development of the organisation's security risk management framework, and ensure there are agreed policies and procedures in place, as well as provide advice to the management line if required.

When identifying specific security roles and responsibilities, you will need to consider what is appropriate and realistic for your organisation bearing in mind its size, the complexity of its structure, existing roles and capacity, and the type of work your organisation does.

Example structure and responsibilities



The Board

- Provides strategic direction and oversight to ensure that security risks are appropriately managed by the organisation.

Executive Director/CEO

- Ultimately responsible for security risk management within the organisation. Ensures resourcing of security risk management and advises the Board of Trustees on security matters.

Programme/Regional Director

- Accountable for security risk management within their respective programmes/regions. Supports countries in implementing the organisation's security risk management framework and ensuring compliance with security policies, etc.

Country Director/Representative

- Responsible for security risk management at country level: e.g. monitoring country-level risk, and establishing and maintaining appropriate security plans/arrangements for country-based staff. Ensures that all security incidents are reported and investigated.

All staff

- Responsible for complying with all security policies, procedures and directives, and accountable for their own actions. Must understand security context and ensure their behaviour does not increase risk to themselves and/or others. Responsible for reporting all security incidents appropriately.

Security Working Group

- Responsible for developing and revising security policies, setting minimum security requirements and reviewing the organisation's security practices.
- Supports managers in implementing, and monitoring compliance of, the security risk management framework.
- Ensures crisis management plans are developed, implemented, and periodically tested.

Security Focal Point

- Supports management in promoting staff security and ensuring staff knowledge and compliance with security policies and procedures in place.
- Responsible for gathering reliable security information and keeping staff informed and updated on security issues.

First, you must identify those existing positions that have a critical role in staff security, including managers based at headquarters and in-country teams (if your organisation has a permanent presence in-country). Next, clearly define the security responsibilities and specific decision-making roles that each of these positions should have. These positions and their security responsibilities should be clearly mapped out in the organisation's security policy so that all staff are informed.

Further information

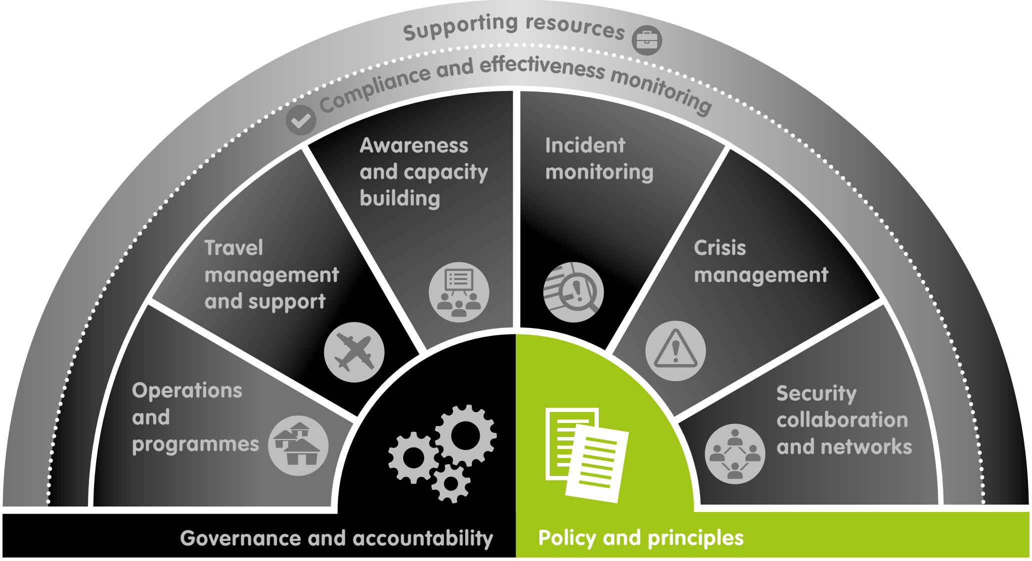
Example Job Description: Logistics and Security Officer

Example Job Description: Field Security Coordinator

Example Job Description: Deputy Director of Global Security

Example Job Description: Director of Staff Safety and Security

4 Policy and principles


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Your organisation's security policy will be the cornerstone of its security risk management framework. Establishing a global security policy will help demonstrate your organisation's commitment to the security of its staff. The policy also provides a clear statement of the organisation's approach to security risks, the key principles underpinning this approach, and the roles and responsibilities that staff members have in managing these risks.

A security policy is a must for all organisations, regardless of size. It informs staff of the principles, approaches and responsibilities for security risk management, and ensures that staff act in a manner that is appropriate for the organisation.

Developing a security policy

When developing or reviewing your organisation's security policy, you must clarify its scope:

- Does it focus on security alone, or security and safety? Some NGO security policies do not include safety as this is already addressed in a separate health and safety policy.
- Who is covered by the policy? While it clearly applies to staff, what about consultants, contractors, volunteers, visitors, accompanying dependants or other associated parties? The policy should address the security of all, making explicit any differences for different groups.

The security policy should be a short and accessible document that is translated into the organisation's core operational languages. Most security policies are structured around four key sections:

1. A **statement** on the importance of staff security and safety, the scope of the policy and who it applies to.
2. A **'principles'** section explaining the organisation's security culture, risk attitude and the key principles that shape the organisation's approach to staff security and safety.
3. A **'responsibilities'** section setting out the organisation's security risk management structure and the roles and actions allocated to specific positions.
4. A **'minimum security requirements'** section establishing the specific organisational security requirements that must be in place; for example, each country must have a security plan.

The security policy is a key governance document which will need to be endorsed by the Executive Director, or a person in a similar position, and then approved by the Board of Trustees. The security policy must cross reference the organisation's other governing policies and codes which outline requirements related to security risk management, such as the health and safety policy, staff code of conduct, whistleblowing protocols, as well as policies on staff wellbeing and care, fraud and corruption, and information security.

Common security principles

- **Shared responsibility** – managing and reducing the risks to staff is a shared responsibility involving staff at all levels within the organisation.
- **Acknowledgement of risk** – managing security will not remove all the risks. Individual staff need to appreciate, as part of their informed consent, that they are still exposed to risk.
- **Primacy of life** – staff safety is of the highest importance to the organisation, and staff should never place themselves at excessive risk in order to meet programme objectives or protect property.
- **Proportionate risk** – the risk to staff must be constantly assessed and should be proportionate to the need for, and benefits of, certain activities, and to the ability of the organisation to manage these risks.
- **Equitable security** – some individuals may be more vulnerable to certain threats than their colleagues. These individuals must be informed of the risks, but security restrictions/measures should not discriminate against individuals based on their personal characteristics.
- **Right to withdraw** – all staff should have the right to withdraw from, or refuse to take up work in a particular area due to security concerns.
- **No right to remain** – the organisation has the right to suspend activities or withdraw staff from situations that it considers to be too dangerous. Staff do not have a right to remain in a location if they have been directed to withdraw from it by senior management.
- **Security strategies** – an organisation's approach to mitigating risk is described as its security strategy. For most NGOs, this will be a balance between 'acceptance' and 'protection', with 'deterrence' as a less common approach.
  📖 *See EISF guide 'Security to go' and ODI guide 'GPR8 – Operational Security Management in Violent Environments'*

The security policy should also clearly explain the organisation's position on weapons and armed personnel, its relationship with armed actors and the use of military resources, as well as its standpoint on ransoms and bribes.

Further information

Organisational Security Policy Framework Example

'Open NGO Security Policy' by the Centre for Safety and Development

EISF guide 'Security to go: a risk management toolkit for humanitarian aid agencies'

EISF guide 'Security Audits'

ODI guide 'GPR8 - Operational Security Management in Violent Environments'

EISF Theme webpage 'Policy, Procedure and Practice in SRM'

Establishing security requirements

Your security policy should stipulate the basic security requirements that the organisation expects to be in place as standard in all locations staff travel to or are based in. For example, should security inductions and briefings be provided to all staff? Is a specific type of security training required to visit or work in certain locations? Do visits to higher risk locations require specific travel authorisation? Are all country offices required to complete risk assessments and develop security plans?

▶ *See 'Security plans' in section 5: Operations and programmes*

> *'Be realistic about the capacity and resources your organisation has available. There is little point in establishing extensive minimum security requirements that your organisation does not have the capacity or resources to provide. Even though a requirement may be recognised as good practice, the credibility of the security policy will be undermined if staff are forced to disregard a requirement because there is not the resource to meet it. That said, certain duty of care standards must always be met, regardless of your agency's resources and capacity.'*
>
> ***NGO Security Advisor***

Given the range of countries and therefore security contexts which your staff work in or travel to, clearly not all countries will require the same level of security measures. Security requirements should be adjusted to reflect the different levels of risk. Systems should, however, be kept as simple as possible to minimise staff confusion and encourage compliance. For example, the policy may state that all staff must have a pre-departure briefing, but the content may change. Therefore, staff going to higher risk environments will require a detailed pre-departure security briefing, and staff travelling to moderate-risk destinations may only require basic travel advice.

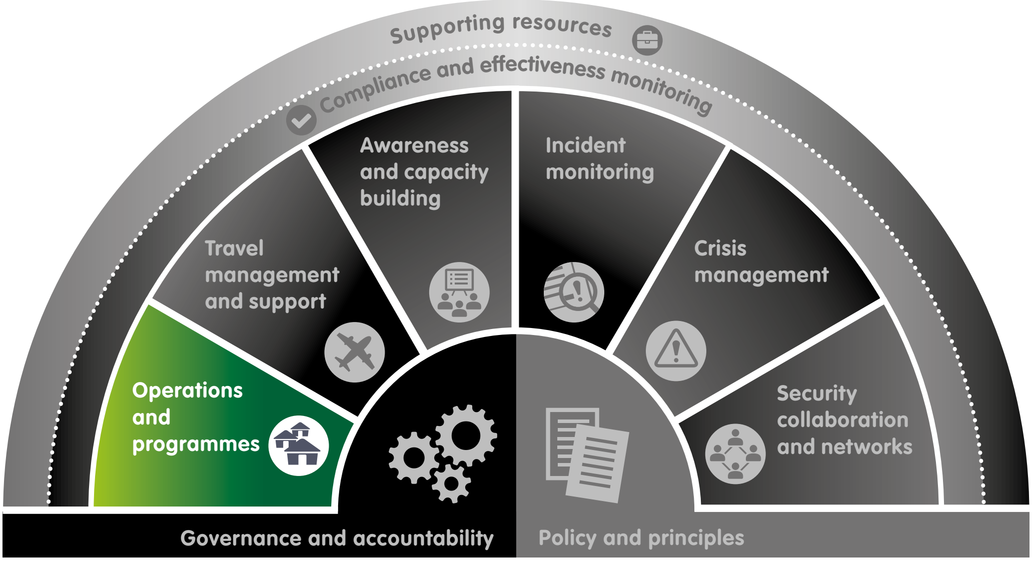
Whether staff are travelling to a country with a country office or are travelling to a partner organisation may also impact on how the policy is implemented.

It is important to note that security requirements alone do not constitute a complete security risk management system; these are the **minimum** required and are the starting point from which to build robust security risk management that reflects good practice and is appropriate for the level of risk faced by your staff.

Further information

'Minimum Operating Security Standards (MOSS)' by InterAction

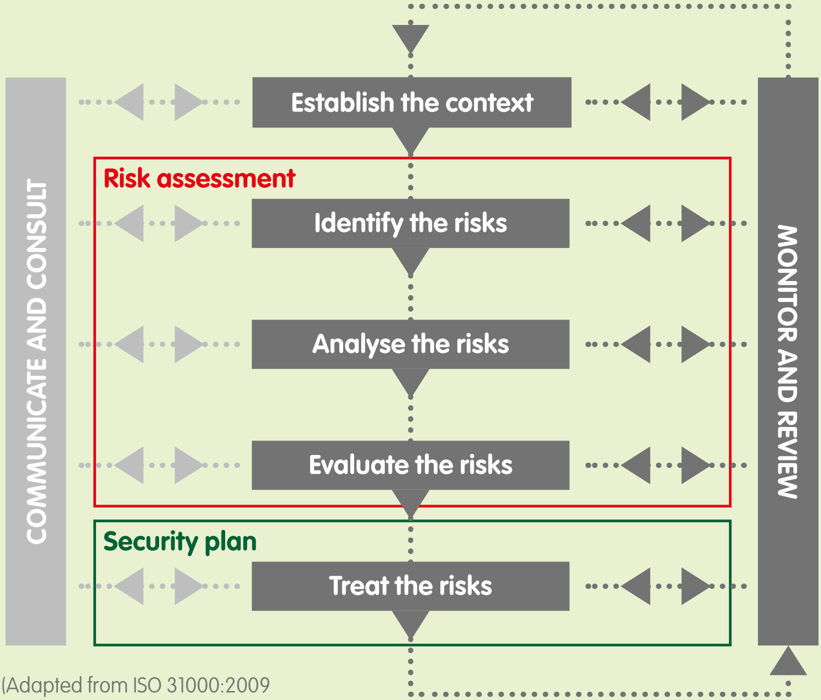
5 Operations and programmes


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Being prepared with realistic plans, procedures and resources is crucial to managing risks in your operations and programmes. You must establish a systematic risk management process that enables managers to analyse the operating environment, identify the risks to staff and operations, and to determine the most effective approaches and measures to manage the risks in that specific context.

> *'It is important to recognise when developing the plans and procedures to manage risks, that the aim is to enable your staff to obtain and maintain safe access to deliver programmes and is not managing security for the sake of security. If it is not possible to put in measures that allow your staff to work within the organisation's accepted risk threshold, the organisation should re-think whether its objectives are appropriate and if it should be working in that context.'*
> ***NGO Security Director***

Risk management process



(Adapted from ISO 31000:2009
Risk Management Process)

There are various risk management process models that NGOs can adopt. For example, ISO 31000:2009, which is an international standard that has been integrated by many NGOs. ISO 31000:2009 defines risk as the effect of uncertainty on objectives, and outlines the following key stages for managing risk:

- **Establish the context** – review both the external and internal context. A thorough grasp of your operational environment and the various stakeholders involved, combined with a detailed understanding of your NGO's impact on the context through the activities and the staff involved as well as your organisation's capabilities, will enable you to appreciate the possible security challenges for staff, programmes, and the organisation.
- **Identify the risks** – identify all possible security and safety threats that could affect staff, programmes or the organisation (including its reputation), and understand how, when and why each threat might occur.
- **Analyse the risks** – undertake a comprehensive assessment to determine staff members' exposure to the different threats identified. You should assess each risk (threat and exposure to it) to determine the severity, considering the likelihood of it occurring and the potential impact should it occur, given the current measures and procedures in place.

- **Evaluate the risks** – with a good understanding of the organisation's risk exposure, you can make informed decisions on whether to accept certain risks or take additional actions to prevent or minimise them.
- **Treat the risks** – options to prevent or minimise/mitigate risk include reducing the risk, transferring the risk to, or sharing it with, other parties, or ultimately avoiding the risk by not undertaking that activity. Reducing security risks involves implementing different strategies that minimise the likelihood and/or impact of certain threats. These strategies are put into practice through the development of country, or area, security plans.
- **Monitor and review** – you must continually review each component of the risk management process to ensure that current approaches and measures remain appropriate to the changing situation.

Effective communication and consultation are integral to the risk management process. No individual can hold all the information needed to identify, analyse and mitigate the risks. It is, therefore, important to identify a range of stakeholders, both internal and external, who can assist you in this process.

The risk management process can also be used as a tool to assess partner organisations that your staff might visit or be embedded in.

Further information

EISF guide 'Security to go: a risk management toolkit for humanitarian aid agencies'

ISO 31000:2009

ODI guide 'GPR8 - Operational Security Management in Violent Environments'

EISF briefing paper 'Security Management and Capacity Development: International agencies working with local partners'

EISF briefing paper 'Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management'

EISF briefing paper 'Security Risk Management and Religion: Faith and secularism in humanitarian assistance'

Upcoming EISF briefing paper 'Managing the Security of Staff with Diverse Profiles'

Security risk assessments

Risk assessments are your insight into the dangers that your organisation, programmes and, crucially, your staff face in a specific location. A security risk assessment is a fundamental element of the risk management process and must be viewed as an integral part of the wider assessments involved in establishing operations or programmes in any country, whether implemented directly or by partners.

Risk analysis matrix

		Impact				
		Negligible	Minor	Moderate	Severe	Critical
Likelihood	Certain/ Imminent	🟨	🟧	🟧	🟥	🟥
	Highly likely	🟨	🟨	🟧	🟥	🟥
	Likely	🟩	🟨	🟧	🟧	🟥
	Possible	🟩	🟩	🟨	🟧	🟧
	Unlikely	🟩	🟩	🟩	🟨	🟨

🟥 Extreme risk	Immediate action required. Is the risk acceptable?
🟧 High risk	Implement specific security and safety measures and contingency plans
🟨 Medium risk	Requires heightened awareness and additional procedures
🟩 Low risk	Managed by routine security and safety procedures

A detailed understanding of the risks in a specific context is essential if your organisation is to make more informed security decisions.

Assessing risk must not be a one-off event. A continuous re-evaluation of all possible risks will help ensure that you have appropriate security measures in place at all times.

The risk assessment process first identifies the different security threats within a given context, and how your staff, assets, the programmes being implemented, or the organisation could be vulnerable. It then analyses them according to likelihood and impact to determine the degree of risk involved. Finally, it identifies and assesses the different options that could be undertaken to manage these risks. Once mitigating measures are identified it is likely there will still be some residual risk, which should be checked against your organisational risk threshold to see if it is acceptable for the programme to continue. If a risk assessment process is carried out and measures are identified but not implemented, an organisation might be exposed as breaching its duty of care.

The security risk assessment process must be documented and include key findings and proposed measures to manage the different risks. Risk assessments must also be updated on a regular basis. In addition, staff will need guidance on what the different likelihood and impact ratings mean in order to analyse more accurately the various threats and to ensure consistency throughout the organisation. For example, does 'likely to happen' mean a weekly or daily event? Furthermore, it is necessary to clarify the extent to which the predicted 'impact' considers the effect on individuals, programme activities, or the organisation as a whole, as these may be different. When considering vulnerability to threats both the specifics of the organisation and the individual should be considered. For example, role, age, gender, ethnicity, nationality and sexuality may all have an impact.

> *'Risk assessments are often perceived as an administrative burden, something to tick off the bureaucratic checklist. As a result, the vital connection between this analysis and programming is lost.'*
> ***NGO Security Advisor***

There is no prescribed format for security risk assessments but there is plenty of good practice guidance available as well as useful tools and templates. The important thing is to provide staff with a standard risk assessment template that is used in all locations, is easy to complete, and captures the essential information.

Documented risk assessments can also provide a strong rationale when requesting resources and funding to implement the security approaches and measures needed to support staff working in a specific context.

Further information

'Module 3: Risk assessment tool' in EISF guide 'Security to go'

'Security Assessment Tool' by ACT Alliance

Security plans

Security plans are key country-level documents that outline the security measures and procedures in place, and the responsibilities and resources required to implement them. Security plans should be established in all locations where your organisation has a significant presence or is regularly engaged. Even in situations where your organisation has no fixed presence but staff regularly visit, or where you have a single representative or small team, a basic document outlining security arrangements and emergency procedures will help ensure that staff understand the measures in place and, most importantly, adhere to them.

If the risk assessment identifies a threat, the security plan must advise staff on how to manage the risk from that threat.

Security plans must remain relevant and accessible documents, should address the specific risks that exist in that location, and, if appropriate, be specific about to whom and where the measures apply, for example, particular ethnic groups in specific regions. Plans should be updated regularly, especially following significant incidents or changes in the operating environment or activities. They should be translated into local languages where necessary.

Country security plan

Key components of a security plan for a country, or specific geographical area, should include:

- **Critical information** – a one-page summary of pertinent information for easy access and quick reference, for example, any restrictions such as curfew times or no-go areas, and important contacts.
- **Overview** – the purpose and scope of the document, who is responsible for the security plan, the organisation's risk attitude, date of completion and review date, and a summary of the organisation's security strategy/policy.
- **Current context** – a summary of the current operating context and the overall security situation, the main risks to staff, assets and programmes (risk assessments system), threats faced in this context, and evaluation of threats and rating of risk.
- **Standard Operating Procedures (SOPs)** – simple and clear security procedures that staff should adhere to in order to prevent incidents, and how to respond should problems arise. SOPs should be linked to the key risks identified and address issues such as cash in transit, communications, incident reporting, field travel and vehicle safety, facilities and site security, office and facility access control, robbery, vehicle accident, personal conduct, staff health and welfare, and information security.

- **Health and safety** – staff protection from health threats as well as accidents, stress and post-traumatic stress disorder.
- **Human Resources** – policies related to recruitment, background checks, contracts, confidentiality, inductions, risk assessment of roles, etc.
- **Security briefings** – what information should be provided to new staff and visitors, and when this information should be provided.
- **Administrative and financial security** – policies for preventing theft, fraud and corruption, as well as cash handling and procurement.
- **Security levels** – the organisation's security levels/phases, with situational indicators that reflect increasing risks to staff in that context and location, and specific actions/measures required in response to increasing insecurity.
- **Incident reporting** – the procedures and responsibilities for reporting security-related incidents, for example, the type of incidents to be reported, the reporting structure, and the format for incident reporting.
- **Crisis management** – members of your crisis management team and activation rules. Include contingency plans in anticipation of foreseeable threats or critical incidents, such as the relocation or evacuation of staff, natural disasters and medical emergencies.
- **Annexes** – additional information, documents and checklists to assist staff in implementing the procedures and plans, for example, contact lists, briefing checklist, and incident reporting form.

Ensuring staff affected by the risks are involved in preparing the security plans will increase the likelihood of them being adhered to because staff will then understand the why rather than just the what.

Further information

'Country Security Plan Example' by InterAction

'Module 6: Security plan' in EISF guide 'Security to go'

Security arrangements and support

Your organisation may have no presence in a country but staff regularly visit, or you may have a single representative or small team there; as a result, staff may rely on local partners or host organisations – each with different security standards and risk attitudes – for security support when visiting programmes or undertaking activities in the country.

Even if you second a staff member to another organisation, you cannot transfer your duty of care responsibilities. As the contracting organisation, you always retain a responsibility to ensure appropriate security and safety measures are in place and are being implemented.

The level and quality of security support available to your staff are determined by what support local partners or host organisations are able, or willing, to provide. It may be that the partner/host is unfamiliar with the risks that your staff are exposed to or the level of support they will need. Risks to staff will increase if the partner/host organisations have few or no security procedures in place, and/or no communication equipment. They may also provide unsafe accommodation and unreliable vehicles.

While the choice of partner or host is clearly a strategic one that is driven by numerous factors, you must also assess the security capacity and arrangements of regular partners or hosts. Where necessary, the partner/host organisation should be supported to develop security plans and procedures and, if possible, you should help them access security training. Also, be prepared to coach these partners and help them provide you with the security information that you and your staff need. Local partners may not have any experience conducting a security risk assessment or developing security plans, but they will certainly possess detailed information on the context that can assist you in assessing the risks and planning security arrangements for your staff.

Even in situations where no formal partner or host is established, staff should always be encouraged to develop relationships with other NGOs in the area, some of whom may be willing to provide information, security updates, and support in the event of emergencies. At the very least, these contacts can provide a 'watchful eye' on staff and be someone to check in with while your staff are in the country.

Partner/host security support

- **Selection** – the process for selecting potential organisations to host your staff should include an assessment of the partner/host's overall security capacity, attitude and approach to risks, local acceptance levels, and existing security procedures and plans.
- **Responsibilities and limits** – make sure that any support agreements are explicit in terms of both parties' security responsibilities and any limitations, in particular on the various responsibilities in the event of security incidents or medical emergencies affecting staff.
- **Security plans and procedures** – ensure partners/hosts have appropriate security plans and procedures, and that these are shared with your staff. If necessary, provide examples or advice to support partners in developing security documents.
- **Information sharing** – maintain a regular dialogue with partners/hosts on the security situation to ensure consensus on the level of risks and how best to manage the security of your staff. Partners/hosts should be requested to share relevant incident reports with your organisation.
- **Networking** – partners/hosts should be encouraged, and if required, supported to link up with local security networks and information sharing mechanisms (for example, those coordinated by INGOs or the United Nations (UN)).
- **Security funding** – in higher risk contexts, it may be necessary to provide partners/hosts with additional funding to ensure essential security resources are in place.

Further information

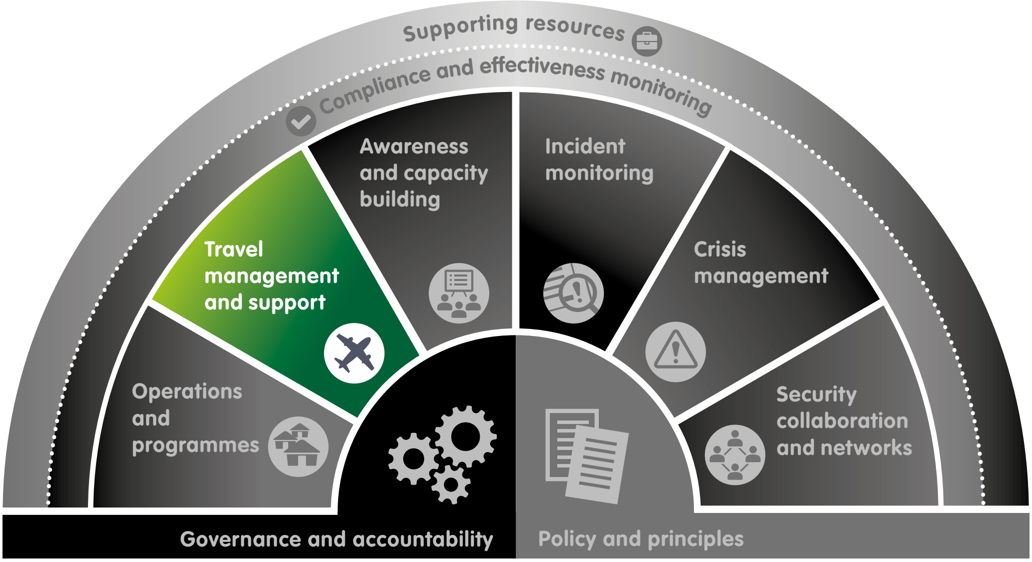
'The Security of Lone Aid Workers' by Gonzalo de Palacios

EISF guide 'Office Opening: A guide for non-governmental organisations'

EISF briefing paper 'Security Management and Capacity Development: International agencies working with local partners'

'Humanitarian Safety and Security: Obligations and responsibilities towards local implementing partners' by Christopher Finucane

6 Travel management and support


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Travel is a necessity for many NGO staff. Whether visiting programmes or attending meetings and events, staff regularly travel to areas of the world with risks that may be unfamiliar to them, or with higher levels of inherent risk. Whenever staff set foot outside their regular working environment, their exposure to various security, safety or health risks often increases, as does their organisation's duty of care responsibilities. This means that security risk management must be a key part of every organisation's overall approach to travel management.

Effective travel security risk management is an ongoing process that starts before departure, continues throughout the time the traveller is at their destination and goes on after their safe return.

Travel risks for staff can be further exacerbated in countries where there is little or no organisational presence. Limited contextual knowledge and up-to-date information on current threats, combined with a lack of security plans or networks, increase the risks for travelling staff.

When planning travel, it is vital that staff and visitors are fully aware of the risks they may face and have been briefed accordingly. Appropriate security and safety measures must not only be in place prior to their travel, but adequate support (including security briefings, secure accommodation, safe transportation, appropriate medical care, etc.) should also be available to them on arrival, while they remain in country, and on their return.

Determining travel risks

Of course, the level and types of risk to travellers will vary significantly according to their destination, the nature of their trip, and their personal profile. Not all locations and journeys will require the same security measures. If your organisation's security risk management framework is not flexible enough to account for the different risk exposures in the various locations staff travel to, there is a risk that existing procedures and measures will be perceived as burdensome or ineffective, or a hindrance to operations, and staff will be reluctant to comply with them.

Access to an up-to-date country risk rating system enables your organisation, and individual staff, to quickly determine the overall level of risk in a specific country or location. Based on this risk rating, you can specify what security measures are required prior to travel, and what level of travel authorisation is appropriate, in line with the organisation's security policy or travel security procedures.

While some larger organisations are able to maintain their own country risk ratings, this requires significant capacity, particularly in order to obtain the necessary information to keep these regularly updated. It may be more effective for your organisation to make use of the travel risk ratings provided by an external security information provider, for example, a company linked to your travel insurance or travel booking service, if available. Alternatively, various open source travel risk ratings are available via embassy travel sites or other website providers.

▶ *See 'Security information and analysis' in this section below*

Example country risk ratings

Country or area risk ratings tend to be based on a four- or five-tier categorisation. Ratings are formulated by assessing several types of risk including conflict, political/civil unrest, terrorism, crime, health and infrastructure. The example below outlines some of the broad indicators used.

Low	Countries or areas are generally secure and the authorities maintain adequate security. There are low violent crime rates and some political violence or civil unrest during elections or other significant events. Acts of terrorism are rare. Risks associated with natural disasters are limited and health threats are mainly preventable. Basic personal security, travel and health precautions are required.
Moderate	Countries or areas experience periodic political unrest or violent protests. Anti-government, insurgent or extremist groups are active with sporadic acts of terrorism. Staff are at risk from common and violent crime. Transport and communications services are unreliable and safety records are poor. The country is prone to natural disasters or disease epidemics. Increased vigilance and routine security procedures are required.
High	Countries or areas have regular periods of political unrest or violent protests, which may target or disrupt foreigners. Anti-government, insurgent or extremist groups are very active and pose a threat to the country's political and/or economic stability. Violent crime rates are high and targeting of foreigners is common. Infrastructure and emergency services are poor and there may be regular disruption to transport and communications services. Certain areas are inaccessible or off-limits to foreigners. Aid agencies may be subjected to threats and harassment by authorities, military or non-state armed actors. Countries or areas are experiencing a natural disaster, or a disease epidemic is considered as high risk. There is a persistent risk to staff, and a high level of vigilance and effective, context-specific security precautions are required.
Extreme	Countries or areas may be undergoing an active conflict or persistent violent civil unrest. The risk of being caught up in a violent incident or attack is very high. The government may have lost control of significant portions of the country, and law and order may have broken down. The lines between criminality and political and insurgent violence are blurred. Foreigners are likely to have no access to significant parts of the country. Transport and communication services are severely degraded or non-existent. The level of violence presents a direct threat to the security of staff. Stringent security precautions are essential and may not be sufficient to prevent serious incidents. Programme activities or movements may be suspended or staff may be withdrawn at very short notice.

Specific travel risk assessments should be completed for staff travelling to higher risk destinations, or where the nature of the visit raises security issues. You need to provide clear guidance to staff when a travel risk assessment is required and clarify who is responsible for approving the assessment and authorising travel. A travel risk assessment form should log the travel destination, travel itinerary, and the traveller's details and experience. In addition, it should assess the overall context and the key security risks in the different locations to be visited, and the specific arrangements in place to manage them.

Further information

Travel Risk Assessment Form Example

Travel security procedures

Many smaller NGOs do not have permanent country offices but staff travel extensively. For these organisations, travel security procedures must be a priority. Travel security procedures outline your organisation's approach to managing risks to staff (and others) when travelling on behalf of the organisation. While security plans mainly focus on locations where your organisation is present or frequently engaged, travel security procedures should cover all locations to which your staff travel, including places where your organisation has little or no presence, and including areas where you work with, or are hosted by, a local partner organisation. The procedures should also include measures for keeping a record of staff locations in lower risk countries where there is, nonetheless, a threat of a multi-casualty event, such as European capital cities.

Staff are more likely to abide by travel procedures if they have had an input in their development and understand the reasons for them.

Travel security procedures may already exist as part of your organisation's wider travel policy. If this is not the case, travel security procedures must be clearly outlined in a stand-alone document; this should address all types of travel conducted by staff and other stakeholders, and provide details of the security measures and what the organisation expects of travellers before, during, and after their trip. Governments may support the evacuation of their nationals in case of political or security unrest although this is not guaranteed and will vary. Any response will be based on the nationality of the individual and not on the headquarters of the organisation. Understanding how the home governments of all your staff would respond in case of a crisis should be checked before an incident occurs.

Travel security procedures

A basic travel security procedure should include:

- **Introduction** – clarifies to whom the procedures apply. Any differences in travel security requirements or support provided to staff, consultants, partners, and official visitors must be highlighted.
- **Travel risk ratings** – explains the travel or country risk rating system used, how staff access the information, the different categories and indicators used, and their implications.
- **Roles and responsibilities** – clarifies the responsibilities of travellers, their line managers or contact points, and senior management in regards to travel security, and how this changes for destinations with higher risk ratings.
- **Travel authorisation** – stipulates who in the organisation authorises travel, the various compliance measures required, and how this changes for destinations with higher risk ratings.
- **Travel risk assessment** – explains when travel risk assessments are required, the template that should be used and who approves the completed assessments.
- **Pre-travel information and briefings** – outlines the information that must be provided to all travellers prior to departure, the type of briefing required and who provides it, and how these requirements change as risk ratings increase.
- **Security training** – explains if security training is required prior to travel and which course must be completed. This may vary depending on the country's risk rating. Information on any training waiver system and who authorises waivers must also be included. It is important to note, however, that duty of care requires a justification for a waiver.
- **Staff/traveller profile forms** – staff, as well as others who are travelling for the organisation, should complete a staff/traveller profile form. Information collected should include personal details (name, nationality, religion, languages spoken, physical identifiers/marks, etc.), emergency contacts (next of kin and/or alternative contacts), medical details (pre-existing health issues, regular medication, blood type, doctor's contact details, etc.), social media footprint (main social media platforms used, in case of critical incidents), and proof of life questions (in contexts where there are abduction/kidnapping risks). Profile forms must be easily accessible outside of normal office hours.
- **Check-in protocol** – specifies with whom travellers must maintain contact while travelling and how often, as well as the escalation process in case of loss of contact. The frequency of check-ins should reflect the increase in the risk rating for the destination.
- **Emergency procedures** – outlines the organisation's emergency procedures for security and medical emergencies including whom to contact, and how to contact them.

Travel security procedures should also specify what happens when staff add personal travel to their work trip in order to cover issues such as insurance, check-in, actual travel times, etc.

'Key information on travelling staff, such as the medical insurance provider, should also be provided, where possible, to the in-country host as in an emergency, the delay in accessing this information from headquarters can have a huge impact on the outcome of an incident.'

NGO Security Director

Security information and analysis

All staff and others travelling on behalf of your organisation should have access to detailed and up-to-date information and guidance on security, safety and health risks associated with their destination prior to departure. For NGOs with little or no country presence, information is available through various government travel advice sites and other open source news and travel information websites; however, it requires substantial staff time and effort to source and collate good quality analysis. Even then, the information available does not always reflect current events or the situation on the ground, and the advice is often focused towards individuals travelling to those countries for business or tourism, rather than NGO staff.

Many organisations make use of external security/travel information services, either through their travel insurance (as a free service or for additional cost) or directly from specific providers. Most external providers offer detailed country and city travel information and reports via interactive online platforms, and include information and advice on significant events that have implications for personal security or are likely to result in travel disruption. However, the quality and depth of the information available from different providers vary significantly, and more in-depth analysis tends to be linked to premium services. If your organisation is looking to make use of external security information services, it is advisable to trial several online platforms and different services before deciding which one to use and whether to purchase premium services. Consider accessing and joining non-profit initiatives such as the Aid Worker Security Database run by Humanitarian Outcomes or the Aid in Danger project by Insecurity Insight, which aim to collect and disseminate information on security incidents experienced by aid organisations. NGO security coordination bodies (e.g. EISF, INSO, etc.) can also help organisations access NGO-specific information.

Selecting external information providers

If considering making use of external security information services, bear in mind the following:

- **Insurance** – identify what security information and support services are already available to staff through your organisation's existing insurance provision.
- **Services** – find out what information and travel support services each provider offers, and consider if this would meet your risk profile and needs.
- **Reputation and experience** – speak to other organisations to ascertain how experienced and credible the various security information service providers are when it comes to their analysis and the information and/or advice they provide.
- **Costs** – consider which providers offer the best value for money in terms of range and quality of services for the cost.
- **Multi-providers** – decide whether to centralise services through one provider, to make use of existing services in addition to buying others or consider local country-specific services. However, using multiple providers to access different information can be confusing and may result in services being underutilised.
- **Online platforms and apps** – check how accessible security information services are, as staff are more likely to make use of a service if it is easily accessible via mobile apps or via websites that travellers are already using such as online travel booking sites.

Travellers and staff must be informed as soon as possible about incidents and events that occur in the country which may have a bearing on their security. Most security/travel information service providers issue email and SMS alerts and advice as situations develop. Some of these alerts services are included in providers' standard packages, but some charge extra for this service. To receive these alerts directly, individual staff need to be registered and either choose to receive alerts based on country selections or have their travel plans linked to the service through a travel booker.

Some providers have developed mobile apps to enable easier access to their information services and for travellers to receive security alerts on their phones. Some providers include access to these mobile apps in their standard packages, while others charge extra for this service. It is important to note that these services are not necessarily geared towards NGO staff. The announcements and advice that these providers issue should be vetted by the organisation and, if necessary, additional guidance should be provided to staff.

Security briefings

Staff and visitors embarking on travel should receive a security briefing specific to the country or area before departure and also on arrival, given by the organisation itself where it has a country presence, or by a partner organisation.

It may not be realistic for your organisation to provide all travelling staff and visitors with a detailed face-to-face security briefing. Therefore, it is important to link briefing requirements to a country/travel risk rating system to ensure that those travelling to higher risk contexts always receive a detailed security briefing. Nonetheless, all travellers should at least be provided with information on the key threats and the precautions to take to avoid them.

Security briefing checklist

- **Current situation** – provide an overview of the current security situation, including key actors and groups, causes of unrest/conflict, state of law and order, levels of crime, and specific areas affected.
- **Security risks** – draw attention to the main security threats to staff, any recent incidents and how staff should avoid them or respond. In addition, draw attention to any security concerns or risks to individual staff associated with their nationality, ethnicity, gender identity, sexual orientation, or disability.
- **Health and safety** – highlight the main natural hazards and health risks in the country or certain areas, the basic precautions staff should take, and how to respond to health concerns or medical emergencies.
- **Personal conduct and behaviour** – highlight all important local laws, cultural norms and customs, and stress what behaviour is expected from staff.
- **Travel and movements** – explain the identification and travel documents required for movement within the country or certain areas, the authorisation process and any movement restrictions (for example, curfews, no-go areas).
- **Communications** – explain the systems used to maintain contact with staff and what will happen if they miss a pre-arranged contact point, as well as any security concerns or restrictions related to communications.
- **Accommodation** – provide an overview of the accommodation and key security measures in place.
- **Key contacts** – provide staff with essential contact information, and ensure they understand how and to whom they must report incidents or problems.

Frequent travellers may consider that they do not require these briefings – but, despite their experience, these staff may be more at risk, as contextual and threat changes may not be immediately obvious to them.

Context-specific security briefings should provide travellers with up-to-date information and guidance for security, safety, and health risks so that travellers understand the local situation sufficiently to operate safely within it.

Further information

EISF briefing paper 'Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management'

Travel monitoring

You must be able to keep in touch with staff and others travelling on behalf of your organisation and monitor their movements. The frequency of contact required will depend on the level of risk in that location. In most cases, this will simply involve a brief phone call or SMS text sent to a pre-defined contact point. Agree on a basic timetable for when staff should maintain contact, and with whom, even if they have nothing to report. At the very least, the organisation should know: that individuals arrived safely; changes to their planned itinerary; when they depart; and that they returned home safely. Staff must be aware of the consequences of missing agreed monitoring points, that is, an escalation process. This escalation must be implemented consistently throughout the organisation or any monitoring system is liable to become pointless.

If a major security incident or event occurs in the country where staff are travelling, your organisation must be able to identify quickly where all staff are and whether they are likely to be impacted. High-tech travel tracking solutions are now more widely available, with many systems able to monitor the precise location of individuals based on satellite/mobile phone GPS. Some staff may be reluctant to be tracked so closely and these high-tech tracking solutions tend only to be a consideration in extreme risk contexts. A more common travel tracking solution, and one that would suit smaller NGOs tracks the broad location of travellers based on their flight bookings. Many travel booking companies and security assistance providers offer travel tracking services; basic services can be free, but the most comprehensive solutions will have an additional cost.

'If you provide staff with an emergency phone number, it is essential that this will be answered promptly 24 hours a day, 365 days a year. 2 hours for a call back with "I'm sorry, it is Saturday" is not acceptable!'

NGO Aid Worker

Insurance provision

Arranging insurance provision falls between different roles within many NGOs and may not get the level of security consideration it warrants. There is a huge range of insurance options available. Selecting insurance on price alone is dangerous, and a false economy. For example, cheaper policies often have limits on cover offered, and can exclude conflict, unrest and acts of terrorism, and/or certain destinations. They often restrict locations based on your home government's assessments of travel risk. Specific extensions, therefore, need to be purchased to ensure staff are fully covered.

When purchasing or reviewing insurance, make sure the policies being considered fit your travel and risk profile, that the countries and locations that your staff potentially travel to and work in are not excluded, and that staff and others travelling on behalf of the organisation are, at the very least, properly insured for medical assistance. Treating and repatriating a seriously injured staff member, consultant or visitor without insurance is extremely costly. Many insurance companies also include opportunities for training or access to other risk management services that may help to reduce organisational risk, so it is certainly worth discussing with your insurance provider to see what services or support may be available.

While insurance is certainly expensive, the bulk of the cost is for elements of cover that are non-negotiable for the type of work undertaken by NGOs. Therefore, including add-ons such as travel information services and alerts, security evacuation and crisis support, may not add significantly to the overall cost of your organisation's annual premium, but may offer substantial security risk management benefits, especially to smaller NGOs with limited capacity and resources in-country.

Insurance details of travellers should be provided to the in-country host organisation whenever possible, including when visiting your own offices, as travel insurance may be from a different provider than for those based in-country.

Types of insurance

- **International Travel and Personal Accident/Illness** – business travel insurance and accident/illness cover, including medical evacuation/ repatriation cover, for insured individuals (staff and associated parties) travelling on behalf of the organisation. Unless the policy includes 'War Risk' cover, many policies exclude certain threats and specific high-risk destinations (based on government travel advice or list issued by the insurance company), and therefore coverage for these locations/risks may require additional premiums.
- **International Health Insurance** – health benefits and medical evacuation/repatriation cover for international staff (and dependants) based overseas. When staff travel outside the country in which they are based, they will normally be covered by the organisation's travel insurance.
- **National Health Insurance Plans** – local/regional health assistance plans. Availability and extent of cover vary, but most provide refunds for medical expenses incurred by nationally-recruited staff. Where medical evacuation cover is included, it tends to be limited to in-country relocation.
- **Emergency Response and Evacuation Insurance** – non-medical support and evacuation cover resulting from political unrest, conflict or a natural disaster. May be included as part of your main travel insurance package or purchased as additional cover.
- **Special Risks Insurance** – kidnap, ransom and extortion cover (or crisis management cover), which refunds the costs incurred by an organisation in responding to a specific incident. Insurance also includes access to specialist response consultants who can advise and support the organisation in managing an incident.

Further information

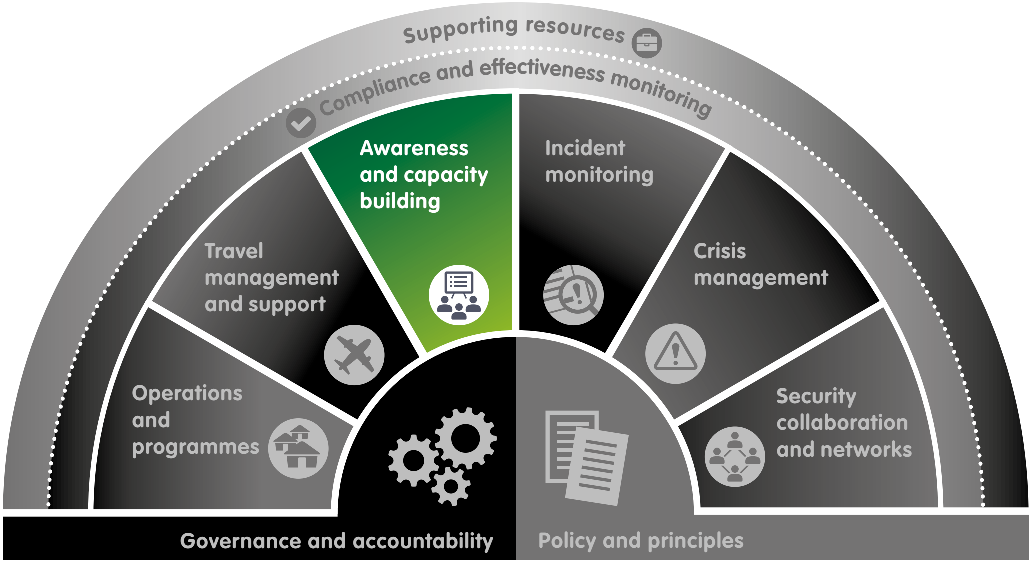
'Guide to selecting appropriate Crisis Management Insurance' by Harry Linnell

'Module 11: Medical support and evacuation' in EISF guide 'Security to go'

'Annex 5: Insurance' in ODI guide 'GPR 8 - Operational Security Management in Violent Environments'

EISF briefing paper 'Engaging Private Security Providers: A Guideline for Non-Governmental Organisations'

7 Awareness and capacity building


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Providing staff with access to appropriate security training that is relevant to their role and the environment in which they are working, combined with continual guidance and support, is an integral part of improving the security awareness of your staff and the security culture of your organisation.

All staff must have the necessary security awareness and skills to enable them to manage their own security as well as that of their colleagues.

Security inductions

Your staff must be adequately informed of the organisation's security policies and approach and be made aware of, and prepared for, the risks and challenges they may face during their work.

Crucial to this is having a security induction process for all new staff members at the beginning of their employment. Ideally, security inductions should be included as part of a wider HR induction process and should orient new staff members to the organisation's security culture, policy and approach, and explain their specific roles and responsibilities in relation to this.

Security induction checklist

- **Security approach** – explain the organisation's approach to security, its risk profile and overall attitude to risk.
- **Policy** – introduce the organisation's security policy, key principles and minimum security requirements, and how these apply in different situations.
- **Security risk management structure** – explain the roles and responsibilities for security within the organisation.
- **Individual responsibility** – highlight each individual's responsibility for their own security and that of their colleagues, the importance of informed consent, and their right to say 'no' if they feel a situation is insecure.
- **Travel security** – discuss the security arrangements in place for travelling staff. Introduce the travel security procedures, and explain the authorisation, briefing, training and travel monitoring requirements in place.
- **Emergency procedures** – explain the organisation's emergency procedures. Inform staff of the medical assistance provider and how to contact them.
- **Incident reporting** – explain what security incidents should be reported and the procedures involved.
- **Additional resources** – familiarise staff with additional security resources, such as guides, handbooks, and training materials.

Security training

Training is a vital part of improving the security awareness and management capacity of staff. Many NGOs understand the importance of security training; in practice, however, cost and availability remain significant barriers to organisations actually implementing and sustaining security training. Smaller NGOs in particular can struggle to resource or justify the expenses involved in providing security training. However, with the increasing development of online security tools and e-learning resources, there is now a wide range of options that organisations can consider when looking to improve the security awareness and capacity of their staff.

Funding for security training should be factored in when formulating project proposals and budgets. Costs associated with security training vary significantly depending on the provider, location, and type of training required.

Types of security training

Security training courses can be divided into four key types:

- **Personal security awareness** – aimed at individuals who work in or travel to moderate-risk environments. Provides basic personal awareness about possible security risks and how to reduce and respond to them.
- **Advanced personal security awareness or Hostile Environment Training (HEAT)** – aimed at individuals travelling to or based in high-risk environments. Provides intensive, threat-specific personal security training, including simulation exercises.
- **Security risk management** – aimed at individuals with security risk management responsibilities (security focal points, programme managers and members of senior management). Introduces the core concepts of security risk management and helps develop skills in security risk assessment, operational security risk management and critical incident management.
- **Crisis management** – aimed at members of senior management or crisis management teams (at headquarters and country levels). Provides awareness of the principles and actions involved in responding to critical incidents or crisis situations. It is delivered as a mixture of live and desktop exercises and/or workshops.

Before you begin to consider security training, you should work out what security training your staff needs, based on where staff work or travel, their roles and responsibilities, risk profile, and the work that your organisation does. For example, there is no point putting staff through an expensive four-day immersive hostile environment course, if they mostly travel to moderate-risk countries for short periods, are based mainly in capital cities, and spend most of their time in meetings or at a hotel.

When conducting a basic training needs analysis, it is important to consider:

- The security competencies and skills required for specific roles and activities within your organisation;
- The level of security experience and previous training that existing staff have;
- The number of staff who require a specific type of security training;
- The geographical spread of staff, and where the security training should be provided to reach the most staff at least cost;
- The budget available and the costs of various training options.

Once you have identified and prioritised the security training requirements within your organisation, you need to consider how best to match these needs with the training resources and options available, which will vary from country to country. Potential training resources include:

- **Online courses.** Several organisations offer free online security courses which provide useful and cost-effective security training resources for staff. While online courses do not offer the same benefits as face-to-face training, they do provide a comprehensive introduction to security and are easy to roll out as a mandatory training requirement for staff.

Online security courses

These are some of the free online courses currently available (all courses require individual registration):

- **DisasterReady.org** – a free online learning platform for aid workers with a number of security courses (including Save the Children and RedR security courses).
- **Kayaconnect.org** – the Humanitarian Leadership Academy training platform, which provides several free online security courses (including UNHCR and Save the Children security courses).
- **IFRC Learning platform** – provides access to the IFRC's *Stay Safe - Personal Security* and *Stay Safe - Security Management* online courses.
- **UNDSS training** – provides access to the UN's *Basic Security in the Field* and *Advanced Security in the Field* online courses.

- **Open courses.** Several external training providers organise regular open courses, in Europe and in regional hubs, which tend to be cheaper than bespoke courses (but your staff will need to travel to the training location). For organisations with resource constraints, using open courses can provide a more sustainable option, as developing and sustaining in-house security training requires significant security capacity.
- **Bespoke courses.** There are a growing number of external providers and individual trainers offering a wide range of bespoke security training courses and services. Many providers/trainers can organise training both at headquarters or country office level. While bespoke security courses tend to be more expensive than open ones, they are more likely to suit the specific security approach of your organisation and the risks that confront your staff.
- **Inter-agency training.** In some countries, inter-agency coordination bodies or the United Nations Department of Safety and Security (UNDSS) - under the Saving Lives Together (SLT) framework - offer security training for NGO staff. If your organisation has staff based in various countries, they may be able to arrange access to these local security training courses at subsidised rates or, in some cases, free of charge.

▶ *For more information on Saving Lives Together see section 10: Security collaboration and networks*

Check that any external training is NGO-appropriate. Many providers and courses are aimed primarily at business travellers, journalists or students and therefore do not address the unique security challenges faced by NGO staff and the approaches needed to manage these risks.

It is advisable to use security coordination mechanisms to find out what external training other NGOs are using. The EISF website provides a list of security training courses, which are advertised only once the training provider has received two separate and positive references from EISF member organisations.

Selecting external training providers

When identifying external training providers, consider the following questions:

- **Profile** – Do their values, motivation, ethics, and culture fit with your organisation and staff?
- **Reputation and experience** – Can they provide references and credible testimonials? Who are their previous and existing clients? Do they have the capacity and experience to provide suitable courses?
- **Content** – What is the training content, approach and methodology? Do they match your risk profile and security approach? Does the training involve simulation exercises? What type of incidents and level of aggression will be used during these exercises?
- **Costs** – Do costs include preparation, travel, delivery, pre- and post-event work? Are costs reasonable and comparative to other providers for the training requested?
- **Trainers** – What skills, knowledge and experience do the trainers have? What is the gender mix of the trainers? Can you request specific trainers?
- **Location and language** – Where will the training take place? How accessible is it for your staff? Are there additional travel costs? What language is required for the training? Do they have trainers who can deliver in the languages your organisation needs?

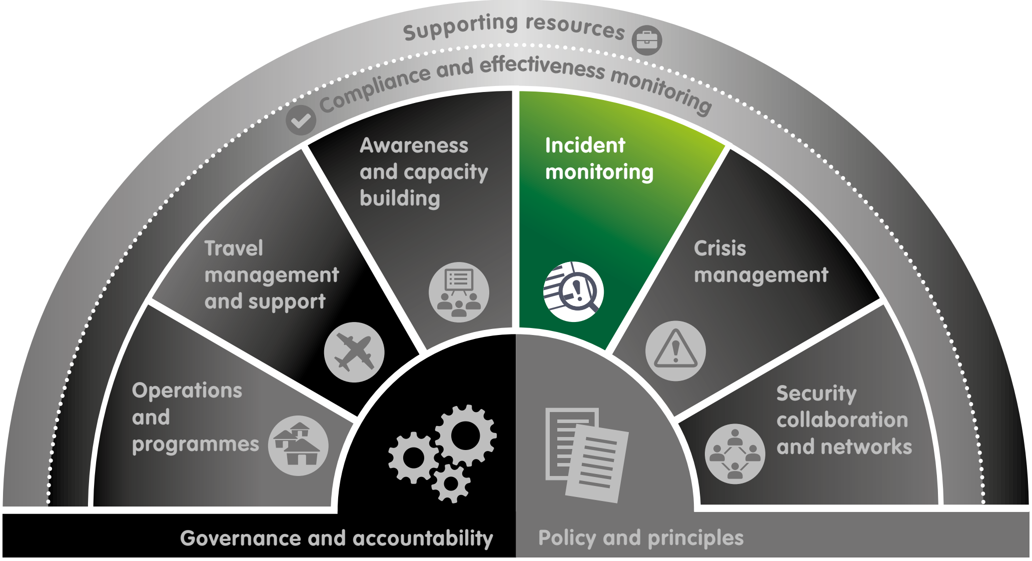
Further information

'NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs' from EISF and InterAction

EISF briefing paper 'Engaging Private Security Providers: A Guideline for Non-Governmental Organisations'

EISF Training and Events webpage

8 Incident monitoring


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Timely reporting of incidents is essential to protect your staff. It ensures that staff receive assistance quickly and that the incident response and its aftermath are effectively managed. A good incident monitoring system will help colleagues avoid similar incidents and react appropriately to changes in the operating environment. It will also improve understanding of the context and support management decision-making.

Regular reporting and monitoring of incidents enables organisations to determine where and how the security situation is changing, why it is changing, and what these changes mean for staff security.

For most smaller NGOs, investing in extensive incident reporting systems and software offers little value, as they are likely to have relatively few incidents to deal with. However, establishing a basic system for reporting and recording security incidents is vital for all organisations, large and small. A basic incident monitoring system consists of two key components:

1. A process for initially reporting an incident or situation;
2. A system for handling the reported information.

Incident reporting procedures

Incident reporting procedures should provide clear guidance on which incidents should be reported, to whom, and the mechanism for doing so.

It is not easy to introduce an incident reporting system into an organisation - it takes time and perseverance for it to take hold and for all incidents to get reported. Under-reporting of security incidents is a challenge in all organisations, so you will need to communicate clearly to staff the purpose, justification and expected benefits of reporting incidents. Better awareness of the need for reporting, trust in how the organisation handles the information, feedback to staff when they report incidents, and an easy-to-use mechanism are crucial in establishing an effective reporting system.

What to report

For many organisations, a security incident is: **any situation or event that has caused, or could result in, harm to staff, associated personnel or a third party, significant disruption to programmes and activities, or substantial damage or loss to the organisation's property or its reputation**.

'Near misses' must also be reported as they may prevent others from being involved in an incident and help staff to understand if and how the security context is changing.

While staff must be encouraged to report all incidents, you will need to be very clear about what a reportable incident is. Perceptions of what is an incident will vary greatly between staff members and locations, depending on what is considered the norm in that context. While you can be confident that major incidents will be reported, there is a risk that staff will overlook or dismiss seemingly isolated or insignificant incidents which, when viewed together, may signify a change in their security situation.

'Near miss' incidents must also be reported. A 'near miss' is an occasion when, either through luck or an appropriate response, a serious incident was avoided.

All serious incidents must be fully examined to understand the events leading up to, during and after the incident. A post-incident inquiry, ideally led by someone not connected with the incident, should consider possible motives or causes, the actions and behaviour of staff, and the response to the incident. Incident investigations should identify key recommendations or follow-on actions, including possible disciplinary procedures, to continually improve security risk management.

Incident reports

As a minimum, reports should address the ***'Five Ws'***: ***Who*** did ***What*** to ***Whom***, ***Where*** and ***When***.

There are typically three types of incident reports:

- **Immediate incident report** – sent the moment the incident occurs or as soon as possible thereafter (when it is safe to do so), normally verbally over the phone or radio, providing a brief summary of what has happened, and any action/support required.
- **Incident updates** – sent as often as necessary, to provide more information on the incident or situation.
- **Post-incident report** – sent after the incident is stabilised or over, providing a written account of the incident and the various actions taken.

Incident report forms

A standardised and easy-to-use incident report form can bring clarity and consistency to your organisation's reporting process. A formal post-incident report should be completed for all security incidents that directly involve your staff or others working on behalf of your organisation. Reports should also be completed following any incident that results in substantial loss or damage to property, or injury or harm to a third party.

A security incident report should provide a complete written account of the incident and the various actions that were taken. A standard template should be created for all post-incident reports.

There will be information that must be treated confidentially, such as certain health conditions, incidents of sexual assault, names of victims, etc. Staff must be provided with guidance on how to handle sensitive or confidential information in order to preserve confidentiality, for example, guidance on who is permitted to access the incident reports, and when and how access to reports should be restricted.

Incident report form

An incident report form should include:

- **Type of incident** – clarifying the type of incident, for example, theft, burglary or armed robbery.
- **Location** – where the incident occurred, using precise locations.
- **Date, day and time** – when the incident occurred as precisely as possible.
- **Who is involved** – who was affected by the incident, including their position, type of programme, nationality, gender, etc., to improve understanding of specific vulnerabilities.
- **Incident description** – a detailed description of the nature of the events, the impact on those affected, and details of any material losses, etc.
- **Incident analysis** – an initial assessment of who may have perpetrated the incident, what caused the incident, whether the organisation or staff were specifically targeted, and the possible implications for the future security of staff.
- **Immediate decisions and actions taken** – information on the decisions and actions taken, and by whom, immediately after the incident.
- **Who has been informed** – a list detailing who the incident has been reported to locally, for example, authorities, other aid agencies, donors or other key stakeholders.
- **Further actions to be taken** – detail the decisions and actions that need to be taken in response to the incident. Give any recommendations for improving staff security.

Further information

Incident Report Template Example

'Chapter 5: Incident reporting and critical incident management' in ODI guide 'GPR8 - Operational Security Management in Violent Environments'

'Guidance Tool F: Good practice in gender-sensitive incident reporting' in EISF briefing paper 'Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management'

Incident logging and analysis

Records of all security incidents should be centralised and analysed periodically. In addition to providing an institutional record of the incident and the organisation's response in the event of litigation or external enquiries, analysing this stored information will allow your organisation to develop a broader, more global understanding of the security issues affecting your staff.

Regular analysis of your organisation's incident reports can be used to:

- Raise awareness of security among staff and therefore strengthen the organisation's security culture;
- Increase understanding among senior managers, and within the Board of Trustees, as to the organisation's risk profile, the main threats that affect staff, and gaps in procedures, support and training;
- Provide analysis to improve decision-making for programme design and implementation;
- Negotiate with insurance providers. Insurers often rely on 'global statistics' to set premiums, but if you can demonstrate the specific risks your organisation is exposed to and the measures you have in place to manage these, you might persuade them to lower their premiums, or at least not to increase them.

There are now several off-the-shelf software packages and open source software tools that can be utilised to record and analyse incident data, and many organisations have established their own comprehensive incident reporting databases. However, for some NGOs, these may seem either too costly or complex to set up and maintain. You may find that using simple Excel spreadsheets to log key information from different incident reports is more than sufficient for your organisation.

It is advisable to share information between different agencies, where possible, in order for your organisation to benefit from a greater understanding of the context - for example, by accessing and contributing to Insecurity Insight's Aid in Danger project and Humanitarian Outcomes' Aid Worker Security Database.

Further information

'Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study' by Gonzalo de Palacios in the EISF briefing paper 'Communications Technology and Humanitarian Delivery'

EISF briefing paper 'Incident Statistics in Aid Worker Safety and Security Management'

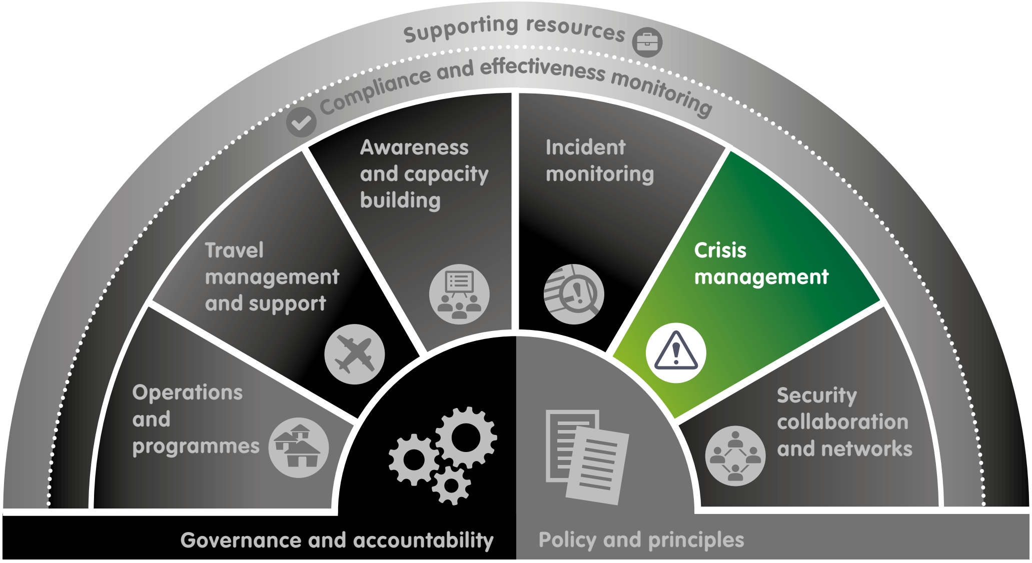
'Managing security information - Simson software' by the Centre for Safety and Development

Aid in Danger Project by Insecurity Insight

Aid Worker Security Database by Humanitarian Outcomes

Incident Dashboard by INSO

9 Crisis management


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

The death, arrest or abduction of a staff member is hugely challenging for any organisation. Not only must the organisation respond to the incident, manage relations with the authorities, and provide support to family and colleagues, but the organisation must still continue to manage its activities and staff in other locations.

The successful resolution and management of any crisis situation depends on your organisation's ability to take appropriate decisions quickly, which requires preparation, a good flow of information, and clear channels of communication that all staff understand.

Preparation is vital for the successful management of any incident, especially where a coordinated, effective response involving different locations and stakeholders is required.

Establishing a crisis management structure

The majority of security incidents will be handled through your organisation's regular line management. However, exceptional situations can arise which, due to the nature and severity of the incident, or its wider implications, would require your organisation to establish a dedicated structure to respond. This is generally referred to as a 'crisis'.

An essential part of pre-planning for such events is to identify a team that will coordinate and manage the organisation's response. A key component of this is the headquarters or regional-based Crisis Management Team (CMT), although the terminology and composition used by different organisations, and their responsibilities, vary significantly. In many cases, the team responsible will consist of key members of an organisation's senior management team. However, roles within the CMT should be determined by the experience, capacity and skills that individuals bring to the team, rather than be solely based on the position that they hold.

It is easier to stand down a CMT when it becomes apparent that the incident is not as serious as anticipated than it is to activate one after the incident has progressed.

You will need to develop a crisis management team and overall structure that suits your organisation. However, good practice based on experience normally includes a small CMT based at headquarters and an incident management team (IMT) based as close to where the incident occurred (or is occurring) as it is safe to be. The strategic decision making authority (DMA) is at the most senior level and external to the CMT. Essential support staff, such as family support staff, a media spokesperson and logistics personnel should be considered as part of the crisis management response structure but are not part of the CMT. It is good practice to identify potential alternative individuals for each of the core roles in order to ensure adequate cover during a prolonged incident response, or where a member is sick, on leave or travelling. However, as a smaller NGO you may find this challenging and therefore you will need to identify a suitable team bearing in mind the capacity, skills and experience you have available.

Crisis Management Team (CMT)

This is a small team dedicated to managing all aspects of an incident or situation and liaising with all the stakeholders involved.

The CMT composition and responsibilities vary depending on the type of incident/situation, its location, and the level of support required.

Core CMT functions	
Crisis Coordinator	Overall coordination and management of CMT and primary decision-making authority within the team. The Crisis Coordinator normally reports to the Executive Director/CEO with whom executive decision-making sits.
Human Resources	Advises on HR policy and coordinates all personnel, family support, and insurance aspects of the critical incident response.
Programmes and Operations	Advises on country context, programme activities, and relevant in-country stakeholders, and coordinates all communication with the country team.
Communications and Media	Advises on media issues and coordinates all media activity and all internal communications.
Information Management and Support	Supports the CMT and maintains information records during the response.

Multiple functions may be carried out by one CMT member. Depending on the nature of the incident, and capacity within the organisation, additional support roles will be required, including security, finance, insurance, legal advice, social media, internal communications, and IT.

The IMT will have similar internal functions as those that are within the CMT, although the focus will be on a more localised management of the incident. Clearly defined and managed communication between the CMT and IMT is essential for the successful response to any crisis. For countries where the NGO has no staff based permanently in the country where the incident occurred, arrangements for how to provide the localised response will need to be included in the crisis management plan.

When is it a crisis?

The point at which an incident or situation becomes critical or a crisis depends primarily on its severity but is also influenced by your organisation's capacity, level of pre-planning and experience in dealing with such incidents.

For some NGOs, less severe incidents or situations may still be considered critical due to the limited capacity, experience and resources the organisation can draw upon to respond. It is usually identified as a 'crisis' when normal management structures are no longer deemed sufficient to cope with the incident, hence initiating the crisis management response.

Any security incident or situation affecting your staff and programmes must be quickly assessed at a senior level to determine its potential impact and to clarify the level of engagement and support required to manage the situation. You should clearly identify what triggers your crisis management mechanism and who in the organisation makes this call. Examples of critical incidents which are likely to activate your crisis management team include but are not limited to:

- Death or serious injury of a staff member;
- Death or serious injury of a third party as a result of actions by staff or the organisation's activities;
- Serious security deterioration or a specific threat that directly affects the security of staff;
- Mass-casualty incident (for example, natural disasters, bombings or attacks) affecting staff;
- Physical assault or sexual violence against a staff member;
- Abduction, kidnapping, arrest or detention involving staff;
- Any security incident likely to result in damaging representation in the media.

Crisis management principles

When responding to any critical incident involving staff, the following key principles must apply:

- Minimise further harm and ensure the security and well-being of the victim(s) and other staff affected by the incident.
- Assure families and other staff members that the organisation is responding appropriately, and provide support to affected family members.
- Minimise possible loss or damage to property and resources; reduce any negative impact on the organisation's reputation and the continuity of existing programmes/activities, so long as this does not put at risk the security and well-being of staff.
- Maintain effective communications with all internal and external stakeholders to enable their cooperation, bearing in mind the need for confidentiality.

Crisis management plans

Every incident is unique and therefore difficult to prepare for fully, but there are essential mechanisms and arrangements that can be planned in advance.

Although a crisis management plan is a headquarters-level document that assists senior management in mobilising and focusing resources in response to critical incidents or crisis situations involving staff, there must also be a country-level component for the local IMT. Clearly defining roles and responsibilities, and developing key action points, checklists and tools as part of a crisis management plan, will enable your staff to respond more quickly and appropriately. Keeping a record of decisions and actions should start as soon as the crisis response mechanism is activated.

Staff will be under significant stress when responding to a crisis, so crisis management plans should be simple to use with easy-to-access checklists.

Crisis management plans

Key components of a basic crisis management plan should include:

- **Introduction** – outline who the document is for, who is covered by the plan, key definitions used, and when and by whom the document should be reviewed.
- **Activation and triggers** – specify how the organisation's crisis response mechanism is activated and closed down, who makes the decision and what criteria are used.
- **Management and decision-making** – outline the structure for managing critical incidents, the key stakeholders involved, the organisation's crisis management principles and confidentiality issues. Include a decision flow chart to explain communication and decision-making.
- **Roles and responsibilities** – outline the specific roles and responsibilities for the different functions within the crisis response structure, including the CMT, IMT and support staff. Terms of reference documents (ToRs) should specify each role's responsibilities before, during and after the incident.
- **Incident protocols** – include procedures and guidance on the possible immediate actions, stakeholder management issues and post-incident support needs that relate to specific incident scenarios, for example, medical emergencies, sexual violence, natural disasters, security evacuations, abductions and kidnapping incidents, and staff death.
- **Resources and tools** – include checklists, formats and tools to support the organisation's response, including templates to log communications and decisions, key contact lists, etc.

Assistance providers and support

Specialist external assistance providers can play a vital role in supporting your organisation during a crisis by ensuring access to specialised knowledge and advice when it is most needed. In some cases, depending on the nationality of the individuals involved, specialist support may also be provided by the home government.

Even larger organisations, with in-house security teams and extensive security capacity, make use of external assistance providers during crisis situations. For smaller NGOs, which may lack the experience in dealing with these types of incidents or the capacity to cover the various CMT roles, establishing access to external assistance in advance of an incident can be a major factor in enhancing the organisation's crisis response capacity.

Organisations can access comprehensive emergency assistance and crisis management support services from commercial providers and consultants through their insurance or by engaging companies and individuals directly. It is important to ensure that any experts used are appropriate for the organisation and have the level of knowledge required. There are a broad range of services available, including medical assistance and medical evacuation support, evacuation of staff due to a deteriorating security situation or natural disaster, access to abduction and kidnap response consultants, and crisis management support and training. When considering additional support, you should be clear on the type of support services that are included through your existing insurance and which response companies provide these services.

Your organisation cannot delegate the management of critical incidents or relinquish its decision-making responsibility to an external assistance provider or other stakeholders. Your organisation must remain actively engaged and is responsible for ensuring that all responses and actions are appropriate. Any external support mechanisms should complement your organisation's own response to a critical incident.

Countries may help to repatriate their nationals in case of an evacuation caused by a security incident (for example, a coup d'état), however, this will be dependent on the country, both host and home, and should not be assumed.

The UN also does not guarantee to evacuate aid workers who are not UN employees. Even if they do carry out an evacuation they are likely to charge the full cost for their assistance.

Further information

Crisis Management Plan Example

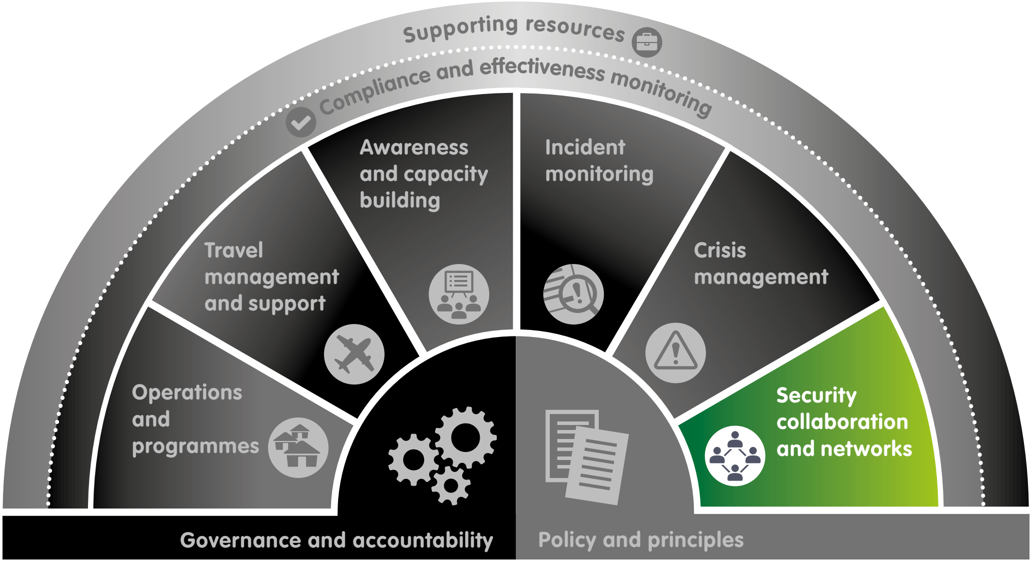
EISF guide 'Managing the message: Communication and media management in a security crisis'

EISF guide 'Family First: Liaison and support during a crisis'

EISF briefing paper 'Crisis Management of Critical Incidents'

EISF briefing paper 'Engaging Private Security Providers: A Guideline for Non-Governmental Organisations'

10 Security collaboration and networks


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

With growing concern for staff security, NGOs are placing greater emphasis on security collaboration and information sharing with other organisations. Access to reliable information, analysis and advice can enhance situational awareness, support better and more informed decision-making, and ultimately strengthen the security approaches of all organisations, large and small. However, security collaboration takes time and investment from staff to make it effective. Ultimately, collaboration mechanisms are only as good as the participation of the organisations involved.

Actively sharing security information and collaborating with other organisations improves the collective security of all.

Inter-agency security networks

In recent years, NGOs have formed various inter-agency security networks and platforms, at country, regional and headquarters levels. These collaborations facilitate the exchange of security information, raise awareness through security training and workshops, and promote good practice. A wide range of mechanisms exists, with varying degrees of formality. These include: informal meetings between a few NGOs to discuss security challenges, dedicated security offices providing information and support to the NGO community in a particular context, and headquarters-level membership networks for security focal points from different NGOs (such as EISF and InterAction).

The range of services provided by such initiatives at country level may include:

- Convening security meetings/briefings;
- Issuing security alerts/threat warnings and advisories;
- Providing regular security reports;
- Preparing analytical reports on incident trends or specific security challenges;
- Liaison with UNDSS and other security actors (national security forces, including police and military, international military forces, etc.);
- Facilitating access to security training and workshops;
- Providing assistance and support during critical situations and incidents.

At headquarters or regional level, services tend to include:

- Convening meetings to discuss security-related issues;
- Facilitating information sharing on good practice for security risk management;
- Supporting organisations to develop appropriate strategies and policies for effective security risk management;
- Liaising with security actors, such as the UN, at a headquarters/strategic level;
- Championing a greater focus on and improvements in aid worker security within the broader humanitarian sector.

European Interagency Security Forum (EISF)

EISF is an independent network of security focal points that represent European-based humanitarian NGOs operating internationally. EISF is committed to improving the safety and security of operations and staff, as well as strengthening humanitarian security risk management in order to achieve greater access to, and impact for, crisis-affected populations.

The EISF Secretariat works in collaboration with its members to produce original research, arrange biannual forum meetings and regular workshops, and facilitate information sharing between members and the wider NGO community. Visit EISF at www.eisf.eu

The timely and reliable security information, advice and support that these mechanisms provide could contribute significantly to the security of your staff. However, as the information and advisories provided by these coordination mechanisms are general for the context and not tailored to a specific organisation, it is vital that you assess how pertinent this advice is to your organisation given its specific profile and capacity. Colleagues with security responsibilities at country, regional and headquarters levels should be actively encouraged to identify and forge relationships with the various inter-agency security networks.

> *'Even if an organisation decides against participating in a formal security coordination mechanism, it should still look to share information and discuss security issues on the ground. As NGOs, we do not work in isolation and therefore our staff's security is very much dependent on the information and support we receive from other organisations.'*
>
> ***NGO Security Focal Point***

At the global level, there are several initiatives that aim to strengthen security collaboration between organisations, including the Saving Lives Together (SLT) Framework, which aims to enhance UN-NGO security collaboration in the field.

Saving Lives Together Framework

Saving Lives Together is a series of recommendations aimed at enhancing security collaboration between the UN security management system and international NGOs/international organisations, and includes:

- Establishing security coordination arrangements and forums;
- Sharing relevant security information;
- Cooperating on security training;
- Cooperating on operational and logistics arrangements, where feasible;
- Identifying resource requirements for enhancing security coordination between the UN, international NGOs and international organisations, and advocating for funding;
- Consulting on common ground rules for humanitarian action.

Further information

'Saving Lives Together - A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field' by IASC

'Guidelines for the Implementation of the "Saving Lives Together" Framework' by Saving Lives Together

European Interagency Security Forum (EISF)

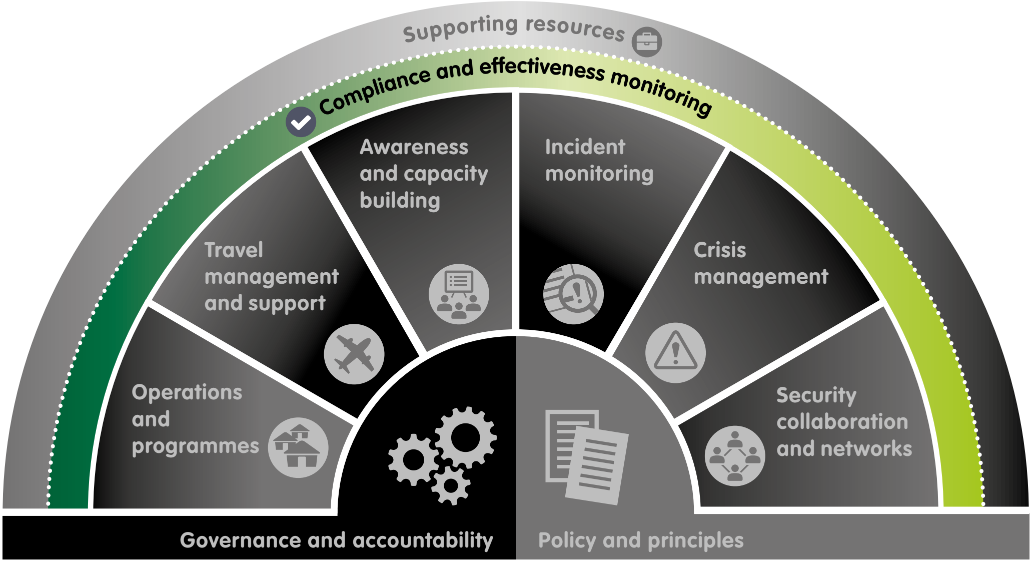
Strategic Security Coordination Mechanisms (EISF theme web page)

The International Safety Organisation (INSO)

International NGO Safety and Security Association (INSSA)

InterAction

11 Compliance and effectiveness monitoring


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

Any initiative to enhance security in your organisation will risk losing support and momentum after it is launched. The risks that your staff face are constantly changing and therefore your security risk management must be continually reviewed and improved.

Security risk management must be responsive to change, both in the external environment and within the organisation. NGOs must regularly monitor and review their security risk management framework to ensure it remains fit for purpose.

Your organisation should monitor compliance, and undertake periodic security reviews and audits, to determine whether policies and procedures are still effective and being followed in practice and that security risks are adequately managed across the organisation to enable access and programme implementation.

Monitoring compliance

So, what are you monitoring? Essentially, you are checking to see that staff are adhering to security policies and procedures and that these are working as expected. Routine monitoring, both of compliance and of the number of incidents that occur, will help ensure that risks are being managed effectively in accordance with your organisation's security framework, policy and procedures. This will also help assess the effectiveness (or example, access, impact, benefits and costs) of your overall approach to security. There are different ways in which to monitor compliance, including:

- **Compliance checklists** – a checklist can assist managers/country representatives in assessing compliance with existing security policies and minimum requirements. While compliance checklists cannot fully replace a comprehensive audit or review, they can assist in monitoring when an organisation is rolling out a security risk management framework on what progress has been achieved and where the barriers are.

  📖 *See 'Tool 3 - Document review checklist' in EISF guide 'Security Audits'*

- **Key Performance Indicators (KPIs)** – creating security-related KPIs can help with monitoring if different elements of the security risk management framework are being implemented and are effectively minimising risks to staff. Examples of KPIs to monitor include: up-to-date security plans (% completed); staff travelling to higher risk destinations provided with security briefings (% successful); staff provided with training (total number); and reported incidents (total number).

  📖 *For more example indicators see 'Tool 6 - SMS Audit worksheet template' in EISF guide 'Security Audits'*

- **Incident analysis** – tracking and reviewing incidents that affect staff will improve how your organisation assesses its risk profile. Understanding which type of incidents occur involving staff, how often, and why, will help identify potential compliance issues or gaps in procedures, support and training.

  ▶ *See section 8: Incident monitoring*

If compliance levels are low, you may need to get tougher with offenders. However, poor compliance could be a warning that staff find some parts of your security risk management framework, and the procedures in place, not practical to implement. These will need to be reviewed and adjusted as part of the continuous improvement of your organisation's security risk management framework.

Security audits and reviews

While compliance monitoring uses routine checks, you will need to carry out a more detailed security audit or review at some point. A security risk management audit is an internal or external evidence-based review of an organisation's security risk management framework and its implementation, and assesses whether the organisation is meeting its duty of care responsibilities to staff.

There are two types of security risk management audits:

- **Organisational audits** that review the security risk management arrangements across the whole organisation;
- **Country/location audits** that review the security risk management approach and systems in a specific country or area, often in response to increasing insecurity or changes in the operating environment. These audits need to be carried out in accordance with organisational level policies and not in isolation.

The aim of the audit or review should be to examine the effectiveness of your organisation's approach to security risk management for achieving your programme objectives and to develop an action plan to enhance the security and safety of all personnel. Ensure that you draw on a wide pool of staff for the audit/review (particularly 'risk owners', i.e. those with responsibility and accountability for security risk management decision-making), not only to assess your staff's awareness and understanding of the systems in place but also to allow them to highlight the security risks and challenges that they are confronted with during their work.

In order to obtain an unbiased opinion and benchmark your organisation against other NGOs, or because of your limited capacity, it may be useful to use an external consultant to carry out the security audit or review. Undertaking an external review is a significant cost and getting the most out of the process is essential.

An alternative to using a consultant may be to work with another NGO and undertake a peer review process.

Ensure that the findings and recommendations are communicated to those who participated, and also to the wider staff. Sharing these outcomes with staff not only supports transparency but also helps raise awareness of the importance of security risk management within the organisation.

The EISF 'Security Audits' guide's toolkit has been successfully used by many organisations to complete both internal and external audits and can provide a useful benchmark as well as help identify areas at which to target resources.

External security reviews

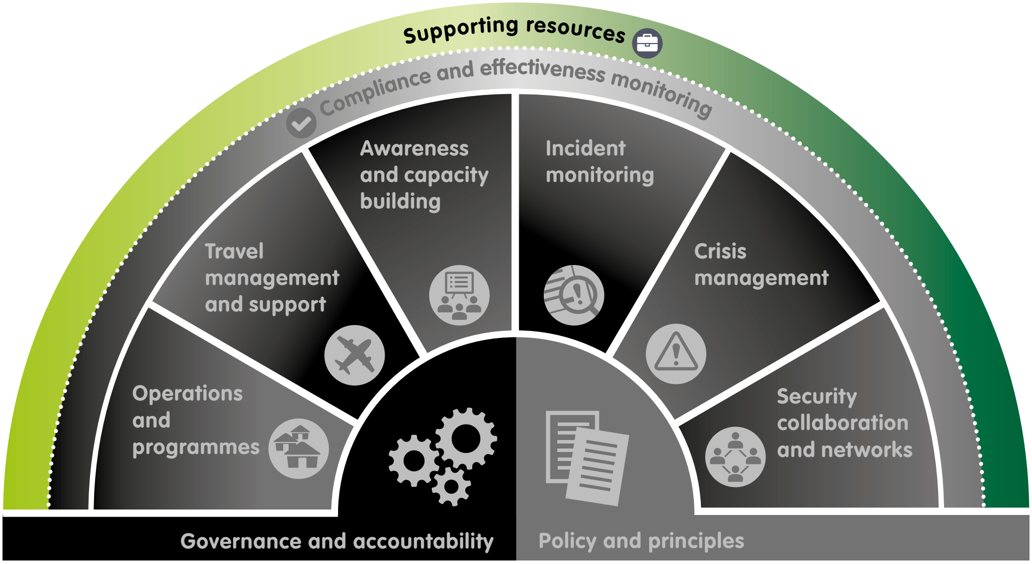
A successful external security review requires the consultant and client to work well together and for both to be clear on expectations and responsibilities from the start. When commissioning an external security review, you should:

- Be sure that there is a genuine need for external support or an independent point of view;
- Draft clear and concise terms of reference (ToR). Be clear about the scope of the review, the deliverables required, and deadlines;
- Be realistic about the timing, the number of days involved, and the budget required;
- Identify suitable consultants through a selection process that is appropriate to the scale of the review;
- Be prepared to discuss your priorities and requirements with the consultant. Confirm all agreements on modifications to the terms of reference in writing;
- Identify a single point of contact within the organisation for the consultant to report to and keep informed on progress;
- Provide the consultant with access to information. Key documents required by the consultant include existing security policies, security risk management guidance, travel procedures, country security plans, crisis management documents, and information on previous incidents;
- Ensure colleagues provide time and materials to support the review. Decide who will arrange the stakeholder interviews and email staff in advance to request their availability and support;
- Manage colleagues’ expectations of the review, circulate the ToR, and develop a practical way to solicit feedback on the report’s findings and recommendations;
- Provide feedback to the consultant on the response to the report and recommendations, and the overall experience of the consultancy.

Further information

EISF guide ‘Security Audits’

12 Supporting resources


Supporting resources
Compliance and effectiveness monitoring
Awareness and capacity building
Incident monitoring
Travel management and support
Crisis management
Operations and programmes
Security collaboration and networks
Governance and accountability
Policy and principles

To strengthen your organisation's security risk management, all managers and staff should have access to relevant security guidance, tools, and templates. An essential component in developing your organisation's security risk management framework is collating, and providing access to, a library of useful security-related resources. Make use of the personal security guidance and NGO security and safety management resources which already exist, rather than reinventing them.

Useful websites

www.eisf.eu

www.eisf.eu/themes

www.eisf.eu/training-and-events/

www.eisf.eu/theme/other-coordination-mechanisms/

www.ngosafety.org

www.ngosafety.org/keydata-dashboard

http://ingossa.org/

www.interaction.org/work/security

www.insecurityinsight.org/aidindanger

https://aidworkersecurity.org/incidents

www.disasterready.org/

https://kayaconnect.org

https://ifrc.csod.com/

https://training.dss.un.org/

Personal security guidance

Stay Safe: The International Federations' Guide to Safer Missions by IFRC (2009).

Safety First: A Safety and Security Handbook for Aid Workers by Shaun Bickley, Save the Children (2014).

Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas by David Lloyd Roberts, ICRC (2005).

Safety Guide for Journalists by Reporters Without Borders and UNESCO (2015).

Security risk management guidance

Security to go: a risk management toolkit for humanitarian aid agencies, 2nd edition by James Davis et al, EISF (2017).

GPR8 – Operational Security Management in Violent Environments, Revised Edition by Koenraad van Brabant, Overseas Development Institute (ODI) (2010).

ISO 31000:2009: Risk Management – Principles and guidelines by International Organization for Standardization (ISO) (2009).

Security Audits by Christopher Finucane, EISF (2013).

Mainstreaming the Organisational Management of Safety and Security (HPG Report 9) by Koenraad van Brabant, Overseas Development Institute (ODI) (2001).

Example documents

Example Job Description: Logistics and Security Officer.
Available from https://www.eisf.eu/library/job-description-example-logistics-and-security-officer/

Example Job Description: Field Security Coordinator.
Available from https://www.eisf.eu/library/job-description-example-field-security-coordinator/

Example Job Description: Deputy Director of Global Security.
Available from https://www.eisf.eu/library/job-description-example-deputy-director-global-security/

Example Job Description: Director of Staff Safety and Security.
Available from https://www.eisf.eu/library/job-description-example-director-of-staff-safety-and-security/

Organisational Security Policy Framework Example.
Available from: https://www.eisf.eu/library/organisational-security-policy-framework-example/

Open NGO Security Policy. Centre for Safety and Development.
Available from: https://www.eisf.eu/library/open-ngo-security-policy/

Security Assessment Tool. ACT Alliance.
Available from: www.eisf.eu/library/security-assessment-tool/

Security Plan Example. InterAction.
Available from: https://www.eisf.eu/library/security-plan-example/

Travel Risk Assessment Form Example.
Available from: www.eisf.eu/library/travel-risk-assessment-form-example

Incident Report Template Example.
Available from: https://www.eisf.eu/library/incident-report-template-example/

Crisis Management Plan Example.
Available from: https://www.eisf.eu/library/crisis-management-plan-example/

Glossary

Acceptance: Building a safe operating environment through consent, approval and cooperation from individuals, communities and local authorities.

Deterrence: Reducing the risk by containing the threat with a counter threat (for example, armed protection, diplomatic/political leverage, temporary suspension).

Crisis: An event that significantly disrupts normal operations, has caused or is likely to cause severe distress, or has severe consequences for individuals, staff or organisations, and requires extraordinary measures to restore order and normality, thus demanding immediate action from senior management.

Crisis management team: A team that manages a crisis situation (i.e. a critical incident) at headquarters or regional level.

Critical incident: An event or series of events that seriously threatens the welfare of personnel, potentially resulting in death, life-threatening injury or illness and triggers an organisation's crisis management response. A critical incident may also be an event that has a serious impact on programmes, organisation assets or reputation.

Duty of care: The legal and moral obligation of an organisation to take all possible and reasonable measures to reduce the risk of harm to those working for, or on behalf of, the organisation.

Protection: Reducing the vulnerability of the organisation to a possible threat, for example, by building walls or hiring guards.

Risk: How a threat could affect the organisation, its staff, assets, reputation or programmes, considering specific vulnerabilities.

Risk assessment: A process through which the organisation identifies the different security and safety threats that could affect staff, assets and programmes, and analyses risks according to the likelihood and impact to determine the degree of risk involved.

Risk attitude: The organisation's approach to assessing and eventually pursuing, retaining, taking or turning away from risk.

Risk management: The coordinated activities that direct and control an organisation with regard to risk.

Safety: Freedom from risk or harm resulting from unintentional or accidental acts, events or hazards.

Security: Freedom from risk or harm resulting from intentional acts of violence, aggression and/or criminal acts against agency staff, assets or property.

Security audit: An internal or external evidence-based review of an organisation's security risk management framework and its implementation, which assesses the effectiveness of the security risk management framework in enabling the delivery of the organisation's objectives, and whether the organisation is meeting its duty of care responsibilities to staff.

Security culture: The 'culture' of an organisation can be simply defined as 'the way we do things around here'. Every organisation has a culture towards security, safety and risks in general.

Security incident: Any situation or event that has caused, or could result in, harm to staff, associate personnel or a third party, significant disruption to programmes and activities, or substantial damage or loss to the organisation's property or its reputation.

Security plan: Key country-level documents that outline the security and safety measures and procedures in place, and the responsibilities and resources required to implement them.

Security policy: A global document that provides a clear statement of 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 these risks.

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

Security strategy: The organisation's overarching approach to security risk management, for example, through an acceptance, protection and/or deterrence strategy.

Threat: Any safety- or security-related or other form of challenge to the organisation, its staff, assets, reputation or programme that exists in the context where the organisation operates.

Vulnerability: The organisation's exposure to a threat. It will vary depending on the nature of the organisation, how it works, what programmes it undertakes, the characteristics of its staff, and its ability to manage risks.

References

ACT Alliance. (2011). *Security Assessment Tool*. EISF.
Available from: www.eisf.eu/library/security-assessment-tool/ [Accessed 25 April 2017]

Behn, O. and Kingston, M. (2010). 'Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management', *Humanitarian Exchange Magazine, Issue 47*. June 2010.
Available from: http://odihpn.org/magazine/whose-risk-is-it-anyway-linking-operational-risk-thresholds-and-organisational-risk-management/ [Accessed 25 April 2017]

Behn, O. and Kingston, M. (2010). *Risk Thresholds in Humanitarian Assistance*. EISF.

Buth, P. (2010). *Crisis Management of Critical Incidents*. EISF.

Centre for Safety and Development. (undated). 'Managing security information - Simson software', *Centre for Safety and Development*.
Available from: https://www.centreforsafety.org/services/simson/ [Accessed 25 April 2017]

Centre for Safety and Development. (2011). *Open NGO Security Policy*. EISF.
Available from: https://www.eisf.eu/library/open-ngo-security-policy/ [Accessed 25 April 2017]

Davidson, S. (2013). *Family First: Liaison and support during a crisis*. EISF.

Davidson, S. (2013). *Managing the message: Communication and media management in a security crisis*. EISF.

Davis, J. et al. (2017). *Security to go: a risk management toolkit for humanitarian aid agencies, 2nd edition*. EISF.

De Palacios, G. (2014). 'Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study', in *Communications Technology and Humanitarian Delivery*. EISF.
Available from: https://www.eisf.eu/library/communications-technology-and-security-risk-management/ [Accessed 25 April 2017]

De Palacios, G. (2016). 'The Security of Lone Aid Workers', *EISF*.
Available from: https://www.eisf.eu/news/the-security-of-lone-aid-workers/ [Accessed 25 April 2017]

Finucane, C. (2011). *Humanitarian Safety and Security: Obligations and responsibilities towards local implementing partners*. Church World Service. Available from: https://www.eisf.eu/library/humanitarian-safety-and-securiy-obligations-and-responsibilities-towards-local-implementing-partners/ [Accessed 25 April 2017]

Finucane, C. (2013). *Security Audits*. EISF.

Finucane, C. (2013). *The Cost of Security Risk Management for NGOs*. EISF.

Garrett, C. (2005). *Developing a Security-Awareness Culture - Improving Security Decision Making*. SANS Institute.
Available from: https://www.eisf.eu/library/developing-a-security-awareness-culture-improving-security-decision-making/ [Accessed 25 April 2017]

Glaser, M. (2011). *Engaging Private Security Providers: A Guideline for Non-Governmental Organisations*. EISF.

Hodgson, L. et al. (2014). *Security Risk Management and Religion: Faith and secularism in humanitarian assistance*. EISF.

InterAction. (2015). *Minimum Operating Security Standards (MOSS).* InterAction. Available from: https://www.interaction.org/document/interaction-minimum-operating-security-standards-and-suggested-guidance-language [Accessed 25 April 2017]

InterAction. (2017). *Security Plan Example*. EISF.
Available from: https://www.eisf.eu/library/security-plan-example/ [Accessed 24 April 2017]

Inter-Agency Standing Committee (IASC). (2015). 'Saving Lives Together – A Framework for Improving Security Arrangements Among IGOS, NGOs and UN in the Field, (October 2015)', *IASC*.
Available from: https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0 [Accessed 10 May 2017]

International Organization for Standardization (ISO). (2009).
ISO 31000:2009: Risk Management – Principles and guidelines.

Kemp, E. and Merkelbach, M. (2011). 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff', *Security Management Initiative*.
Available from: https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/ [Accessed 25 April 2017]

Kemp, E. and Merkelbach, M. (2016). 'Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications', *EISF*.

Available from: https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/ [Accessed 25 April 2017]

Linnell, H. (2017). 'Guide to selecting appropriate Crisis Management Insurance', *EISF*.
Available from: https://www.eisf.eu/news/guide-to-selecting-appropriate-crisis-management-insurance/ [Accessed 25 April 2017]

Merkelbach, M. (2017). *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel*. Swiss Federal Department of Foreign Affairs (FDFA), Stabilisation Unit (SU) and Center for International Peace Operations (ZIF).
Available from: http://www.zif-berlin.org/fileadmin/uploads/experten-einsaetze/Voluntary_Guidelines_on_the_Duty_of_Care_to_Seconded_Civilian_Personnel_Final_170420.pdf [Accessed 10 May 2017]

Persaud, C. (2012). *Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management*. EISF.

Persaud, C. (2014). *NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs*. EISF and InterAction.

Saving Lives Together. (2016). 'Guidelines for the Implementation of the "Saving Lives Together" Framework', *Saving Lives Together*. July 2016.
Available from: https://www.eisf.eu/library/guidelines-for-the-implementation-of-the-saving-lives-together-framework/
[Accessed 10 May 2017]

Singh, I. (2012). *Security Management and Capacity Development: International agencies working with local partners*. EISF.

Source 8. (2015). *Office Opening: A guide for non-governmental organisations*. EISF.

van Brabant, K. (2010). *GPR8 – Operational Security Management in Violent Environments, Revised Edition*. Overseas Development Institute (ODI).
Available from: https://www.eisf.eu/library/gpr-8-operational-security-management-in-violent-environments-revised-edition/ [Accessed 25 April 2017]

van Brabant, K. (2012). *Incident Statistics in Aid Worker Safety and Security Management*. EISF.
Available from: https://www.eisf.eu/library/incident-statistics-in-aid-worker-safety-and-security-management/ [Accessed 25 April 2017]

Annex. **Security Risk Management Framework – quick reference guide**

Governance and accountability

- Determine a suitable security risk management structure for the organisation to enable objectives to be met and ensure there is a clear understanding of roles and responsibilities.
- Identify a Security Focal Point (SFP) to support the development and implementation of the security risk management framework.
- Establish a cross-departmental security working group/committee to oversee the development and implementation of the security risk management framework.
- Ensure that all relevant job descriptions/ToRs outline the security risk management roles and responsibilities associated with that position or activity.

Policy and principles

- Develop a security policy that reflects the organisation's principles and approach to security.
- Ensure the policy clearly outlines the organisation's risk attitude, security risk management structure and the security responsibilities of individual staff and those allocated specific security roles.
- Identify practical and appropriate minimum security requirements that must be in place in each location or activity, linked to a country risk ratings system.

Operations and programmes

- Develop a simple security risk assessment process that identifies key risks in a particular country or location and outlines the control measures in place to manage these risks.
- Ensure that security risk assessments are completed by all country programmes on a regular basis and that these are documented.
- Ensure that security plans, outlining the security measures and procedures in place to manage identified risks, are established in all locations where the organisation has significant presence or is regularly engaged.
- Assess the security capacity and support available to staff from local partners or host organisations. Ensure that any security support arrangements and agreements are clear in terms of both parties' responsibilities.

Travel management and support

- Source a basic country/travel risk rating system to inform staff of the risks associated with working or travelling in those countries. Establish minimum requirements in terms of security measures, mechanisms and training that apply to each risk rating.
- Ensure travel risk assessments are made and approved for all occasions of staff travel to higher risk destinations, or where the nature of the visit raises security concerns.
- Develop specific international travel security procedures for travelling staff, consultants and visitors. These should clarify roles and responsibilities, training and briefings, travel monitoring, authorisations and emergency procedures.
- Ensure staff are provided with detailed, up-to-date information and guidance on security, safety and health risks in their destination prior to departure.
- Make sure all staff, consultants and visitors travelling to higher risk contexts receive a security briefing specific to the country or area they are travelling to, before departure, and on arrival if the organisation has a country office.
- Establish appropriate check-in procedures for travelling staff in order to monitor their movements, and ensure staff can be located based on their flight bookings.
- Ensure that all staff, including consultants, have adequate insurance cover while travelling to and working in the field, and that all staff are fully informed of their insurance provisions.

Awareness and capacity building

- Ensure that all new staff receive a security induction which covers the organisation's security policy and approach, and responsibilities within the organisation.
- Identify suitable online security training resources that should be completed by all staff as part of their induction.
- Review different security and safety training options for different categories of staff based on the risk environments in which they travel and work, and their security responsibilities.

Incident monitoring

- Develop incident reporting procedures and reporting formats. Guide staff on the importance of reporting incidents, what needs to be reported and how.
- Establish a central incident logging system to store key information on all security incidents affecting staff.
- Periodically review all incidents affecting staff to identify potential security incident trends and concerns.

Crisis management

- Identify a suitable crisis management structure to coordinate and manage the organisation's response to critical incidents.
- Develop a Crisis Management Plan which outlines the roles and functions of the CMT and IMT, clarifies decision-making authority, and highlights the key response procedures for crisis situations.
- Consider including access to emergency and crisis management support services (medical and non-medical) as part of the organisation's insurance cover.

Security collaboration and networks

- Ensure that staff regularly participate in inter-agency security forums and meetings in order to strengthen information-sharing and security collaboration.

Compliance and effectiveness monitoring

- Provide managers/country representatives with a security risk management checklist to help them assess compliance with security policies and minimum requirements.
- Ensure that regular country/programme security audits are conducted, especially if activities are undertaken in high-risk countries.
- Undertake a periodic review of the organisation's security risk management approach and framework, and develop an action plan to enhance the security and safety of all personnel.
- Establish and enforce a strong disciplinary culture towards non-compliance with security policies and minimum security requirements.

Supporting resources

- Make available a range of guidance, tools and templates as part of a security library to assist managers and staff in managing security risks.

available at **www.eisf.eu**

Other EISF publications

If you are interested in contributing to upcoming research projects or want to suggest topics for future research, please contact **eisf-research@eisf.eu**.

Briefing papers and reports

Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management – 2nd edition
December 2016
Vazquez Llorente, R. and Wall, I. (eds.)

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. *et al.* Edited by Vazquez, R.

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 – *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Demystifying Security Risk Management
February 2017, (in *PEAR Insights Magazine*)
Fairbanks, A.

Duty of Care: A Review of the Dennis v Norwegian Refugee Council Ruling and its Implications
September 2016
Kemp, E. and Merkelbach, M. Edited by Fairbanks, A.

Organisational Risk Management in High-risk Programmes: The Non-medical Response to the Ebola Outbreak
July 2015, (in *Humanitarian Exchange*, Issue 64)
Reilly, L. and Vazquez Llorente, R.

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose Risk Is it Anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in *Humanitarian Exchange*, Issue 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Security to go: a risk management toolkit for humanitarian aid agencies – 2nd edition
March 2017
Davis, J. *et al.*

Office Opening
March 2015 – *Fr. version available*
Source8

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez Llorente, R. (Sp. and Fr.) – EISF Secretariat

Managing the Message: Communication and Media Management in a Crisis
September 2013 – *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Family First: Liaison and Support During a Crisis
February 2013 – *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L. – EISF Secretariat

eisf

EISF Executive Director
T: +44 (0) 203 195 1360
M: +44 (0) 77 6099 2239
eisf-director@eisf.eu

EISF Research Advisor
T: +44 (0) 203 195 1362
M: +44 (0) 77 6099 2240
eisf-research@eisf.eu

www.eisf.eu

First published / June 2017