eisf

AN EISF GUIDE FOR NON-GOVERNMENTAL ORGANISATIONS

Security to go:

a risk management toolkit for humanitarian aid agencies

EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF)

EISF is an independent network of security focal points who currently represent over 100 aid organisations 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 Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Acknowledgements

The first edition of this guide, published in 2015, was developed jointly by James Davis (Act Alliance) and Lisa Reilly, Executive Coordinator of the European Interagency Security Forum (EISF). The project manager of the first edition was Raquel Vazquez Llorente, Researcher at EISF.

Module 12 – People management was developed by Christine Williamson. The project manager was Adelicia Fairbanks, Research Advisor at EISF.

Module 4 – Digital Security was developed by James Davis. The project manager was Léa Moutard, Research Advisor at EISF.

The European Interagency Security Forum and the authors would like to thank the following individuals for sharing their expertise with us: Marko Szilveszter Macskovich (UN Office for the Coordination of Humanitarian Affairs), Michelle Betz (Betz Media Consulting), Veronica Kenny-Macpherson (Cosantóir Group), Jean Michel Emeryk, Peter Wood, Shaun Bickley, William Carter, Rebekka Meissner, Christine Newton, Rory Byrne and Tom Keunen.

Suggested citation

Davis, J. et al. (2020) *Security to go: a risk management toolkit for humanitarian aid agencies.* 3rd edition. European Interagency Security Forum (EISF).

Disclaimer

Contents

Introduction

About 'Security to go'

'Security to go' is intended to provide a simple, easy-to-use guide for non-security experts to quickly set up basic safety, security and risk management systems in new contexts or rapid onset emergency response situations. This guide is applicable to both international organisations and national agencies moving into new regions and/or setting up new programmes; it is especially applicable to environments where the risk levels have changed due to human or natural causes.

This guide is not an exhaustive examination of all safety, security and risk management systems that can be developed or implemented by national and international organisations working in challenging contexts. Instead, 'Security to go' is intended to give guidance on the key needs that must be addressed in opening a new office, programme or mission. This guide uses checklists and step-by-step tools to ensure important duty of care needs are identified and managed.

The contents of this guide are the results of a collaboration between a number of different types of organisations, individuals and consulting agencies that focus on safety and security issues for international humanitarian organisations. The topics selected for inclusion in this guide represent many key areas but it is hoped additional modules will be added or updated in the future as organisations develop and share their lessons learned in various contexts.

How to use 'Security to go'

This guide can be used in a number of ways. At the most basic level, it can be saved to a memory stick. It can be also printed off and carried by staff deploying into a new context to act as a template for setting up systems and policies at an early stage, and keep staff safe as they set up a programme. Ideally, the document should be considered by management as part of the deployment planning process, programme design planning, or factored into an organisation's scaling up in response to an emergency or significant change to the threat environment.

The following are provided within this guide:

- Crucial activities and tips, indicated with 
- Expert accounts, indicated with
- Cross-references within the guide and to external resources, indicated with
- Key concepts and definitions are listed in the glossary.

For ease of understanding, this guide is organised into three categories of modules: **Planning and preparedness, Response,** and **Support services**.

The planning, preparedness and response modules of this guide correspond to the **security risk management planning process** (see page 7). At the start of each chapter a navigational chart highlights in green which stage of the process will be discussed.

Modules under support services cover areas and processes that affect, complement and feed into an organisation's security risk management and should be considered throughout the security risk management planning process.

The modules are structured to assist staff in developing countermeasures or risk mitigation strategies to counter threats identified in the organisation's risk assessment. Checklists, plans and templates need to be modified to suit each organisation and context.

Security risk management planning process

As with all safety and security measures, the first critical step is to complete a risk assessment. Natural disasters, famines, disease outbreaks and even national elections can present as many risks as human conflict, terrorism or other types of violence. This guide provides a simple risk assessment format that staff can use to identify and measure various risks.

Good security management is not about being risk averse but about recognising the risks and developing appropriate risk management measures to enable the programmes to be delivered safely. If the security measures prevent programmes from being implemented, organisations should consider whether they are equipped to work in those environments.

▶ *See Module 3 – Risk assessment tool*

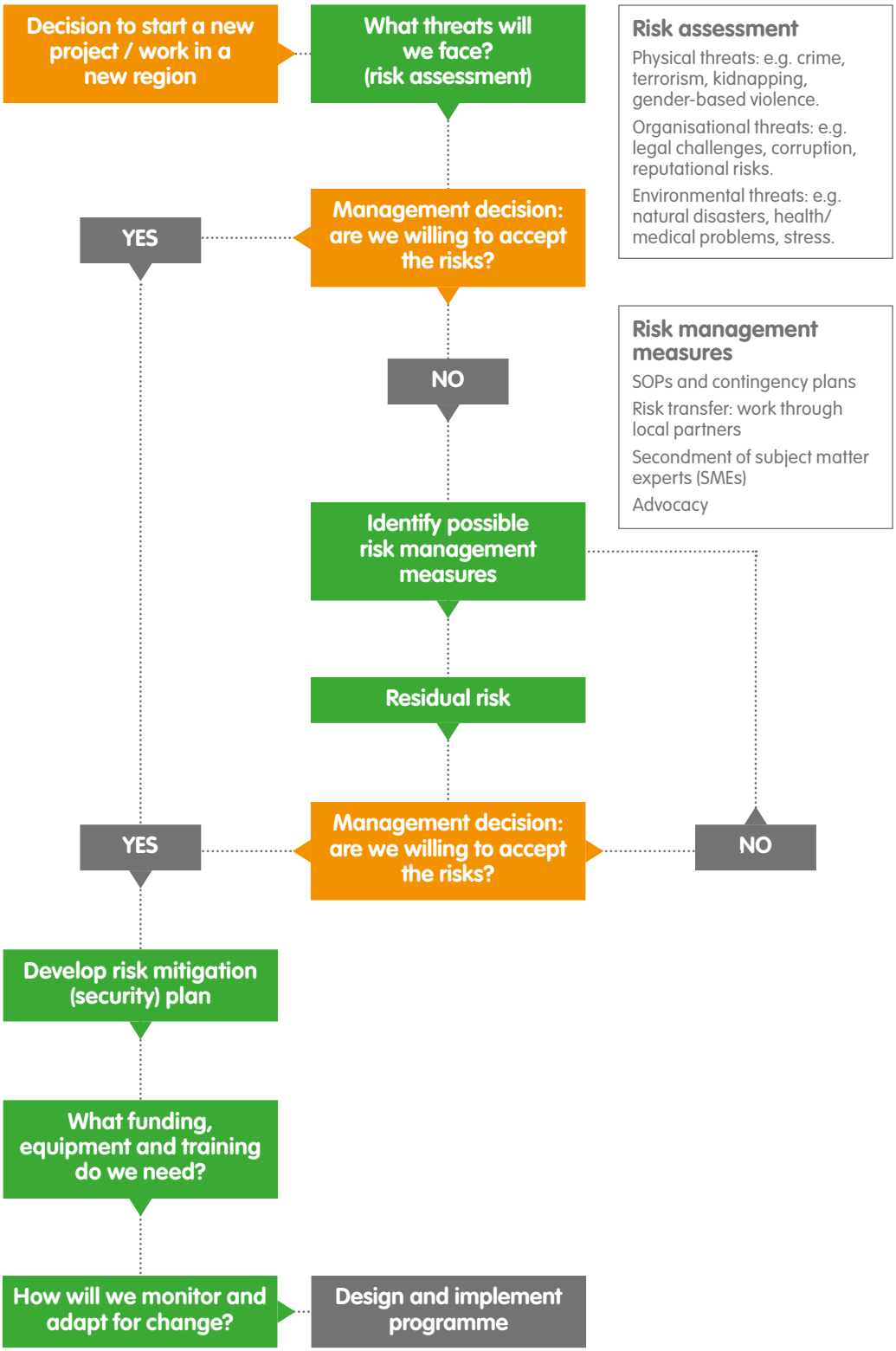
▶ *See Glossary*

Threat

Any safety, security or other form of challenge to your staff, assets, organisation, reputation or programming that exists in the context where you operate.

Risk

How a threat could affect your staff, assets, organisation, reputation or programming.


Decision to start a new project / work in a new region
What threats will we face? (risk assessment)
Risk assessment
Physical threats: e.g. crime, terrorism, kidnapping, gender-based violence.
Organisational threats: e.g. legal challenges, corruption, reputational risks.
Environmental threats: e.g. natural disasters, health/ medical problems, stress.
Management decision: are we willing to accept the risks?
YES
NO
Risk management measures
SOPs and contingency plans
Risk transfer: work through local partners
Secondment of subject matter experts (SMEs)
Advocacy
Identify possible risk management measures
Residual risk
Management decision: are we willing to accept the risks?
YES
NO
Develop risk mitigation (security) plan
What funding, equipment and training do we need?
How will we monitor and adapt for change?
Design and implement programme

In responding to a new emergency, or starting operations in a new region, it is essential to incorporate a security risk assessment into any needs assessment process. By doing so, any security risk management costs can be incorporated into programme design from the outset rather than tagged on at the end.

Duty of care is an increasingly important concept for organisations sending staff into challenging environments. Essentially, duty of care is the legal and moral obligation of an organisation to take all possible measures to reduce the risk of harm to those working for, or operating on behalf of, an organisation. This includes staff, volunteers, interns, contractors (such as guards or drivers) and implementing partner organisations (although the level of duty of care required may be different). NGO organisations, including senior managers and directors on an individual basis, can be sued in many jurisdictions for demonstrating negligence in their duty of care.

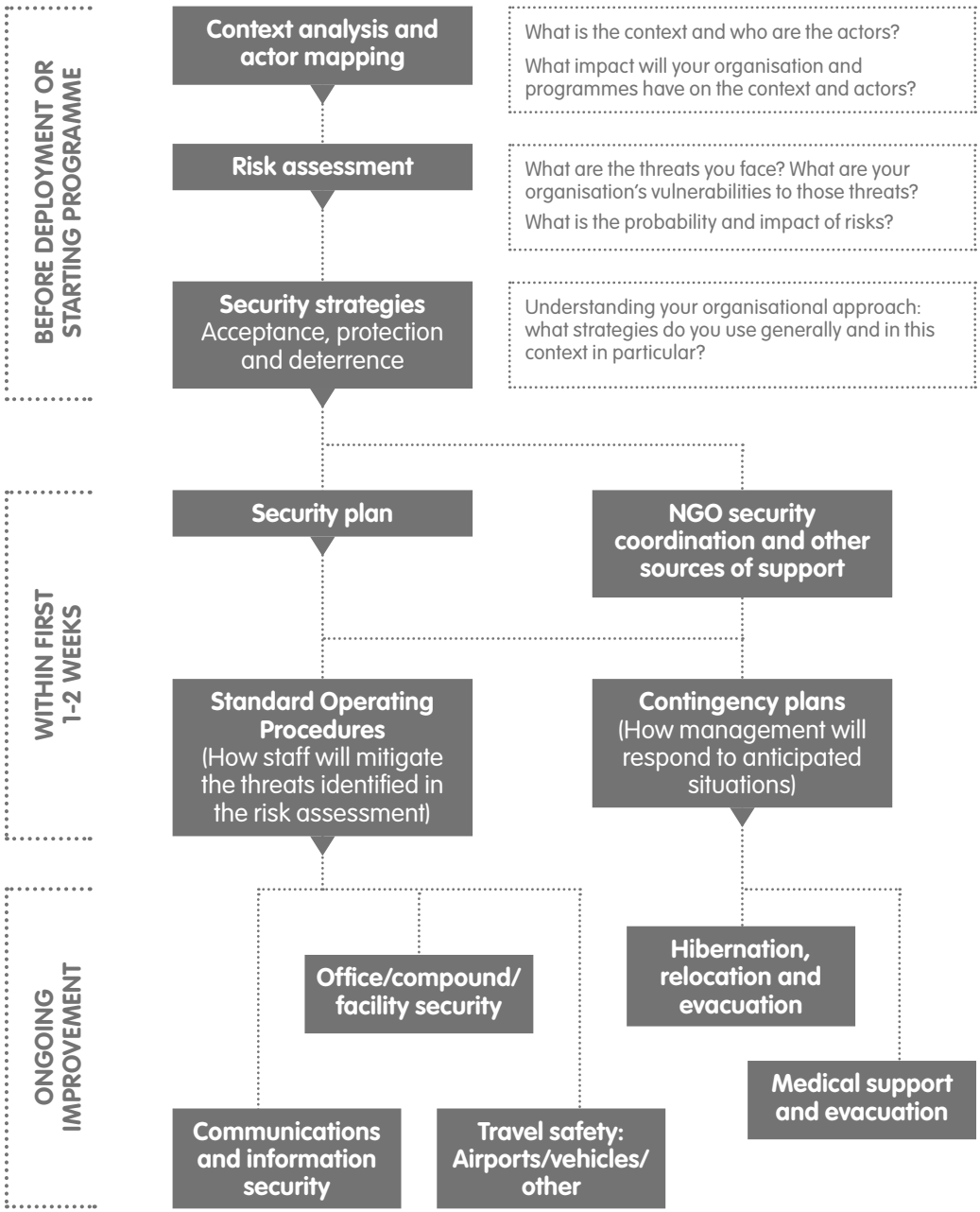
▶ *See Glossary*

Good security risk management doesn't need to cost much financially. In many cases it is more about training staff, creating good policies and constantly monitoring the threat environment. Maintaining an incident map, enforcing a communications check-in policy, vehicle speed limits, emergency supplies or engaging with other NGO forums can cost very little and have a major impact on the organisation's safety and the security of staff and assets. Identifying the responsible staff member(s) and prioritising the time to undertake these activities is the key challenge.

Increasingly donors are aware of safety and security risk management costs. If the risk assessment justifies the expense, direct costs can be incorporated into the programme implementation budget. Necessary security-related costs, such as equipment (radios, satellite phones, first aid kits, emergency equipment/ supplies, emergency cash, facility improvements, insurance or similar), or time (implementing a proactive acceptance strategy, negotiating for sustainable access), can be written into funding proposals. If it is justified by the risk assessment, donors are often willing to fund these security budget lines.

▶ *See EISF report 'The cost of security risk management for NGOs'*

Security risk management planning process



Nothing in life is ever static. Situations improve and also deteriorate. Security policies and procedures need to be regularly updated or adapted to suit changing threats in the operational environment. It is important to define the following:

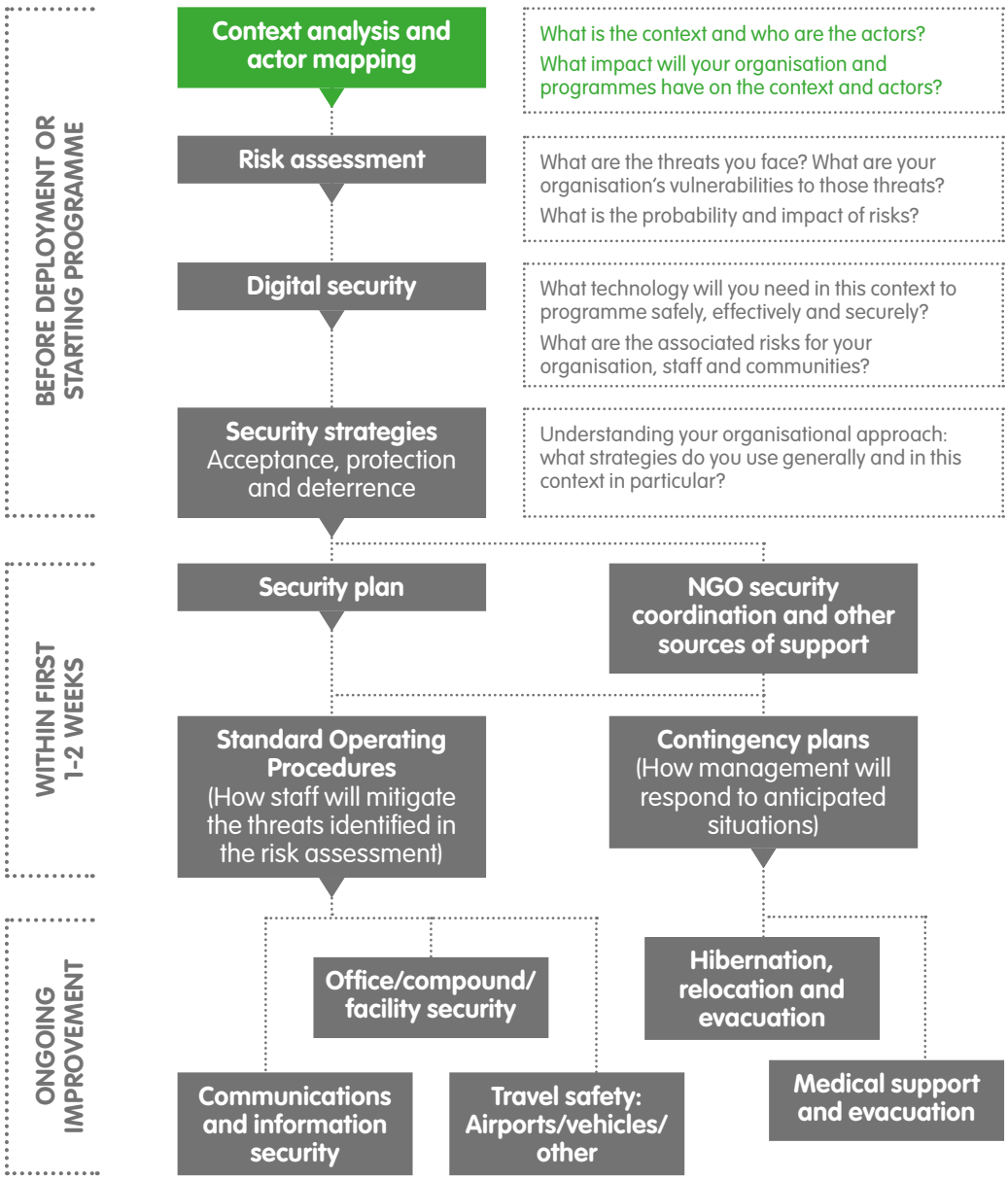
- Who is responsible for reviewing and updating the risk assessment and security plans?
- How often should this be undertaken (annually, quarterly, monthly)?
- How will staff be informed of and trained on changes in policy or procedures?

To monitor the changing nature of the threats in the operational environment it is necessary to identify indicators of change, i.e. what contextual developments can and should be monitored to give early warning of the changes that can have an impact on the risks faced by the organisation.

One of the simplest and best methods for monitoring change is incident mapping, including 'near misses' as well as incidents that have occurred within your operating environment but have not specifically affected your organisation.

By tracking when and where incidents occur, including time of day, who was targeted, and the consequences, it becomes easier to see when the situation is improving or deteriorating. For example, you can use a map with differently coloured pins to represent each type of incident and/or who was involved (your organisation, another NGO, the UN, partner organisation, local NGO).

2 Actor mapping and context analysis



Mapping the different actors in the operating environment and analysing the context are both key activities for organisations moving into a new country/area/region, or starting a new programme or project. It is also essential when a major disruption to the status quo has happened in a familiar operational context.

In recent years, NGOs have been ordered out of countries, or their staff sentenced or imprisoned, despite the state's urgent humanitarian needs, because someone made a simple social mistake, offended a host government, or started work without properly gaining acceptance by both formal and informal leadership structures. It is strongly advised to start an actor mapping and context analysis as early as possible and continue the process throughout the programme duration.

Who are the key individuals, groups, organisations, state institutions and other stakeholders that can affect your security and operations? What is their political and/or social position, power, background and relation to or interest in the organisation?

Actor mapping

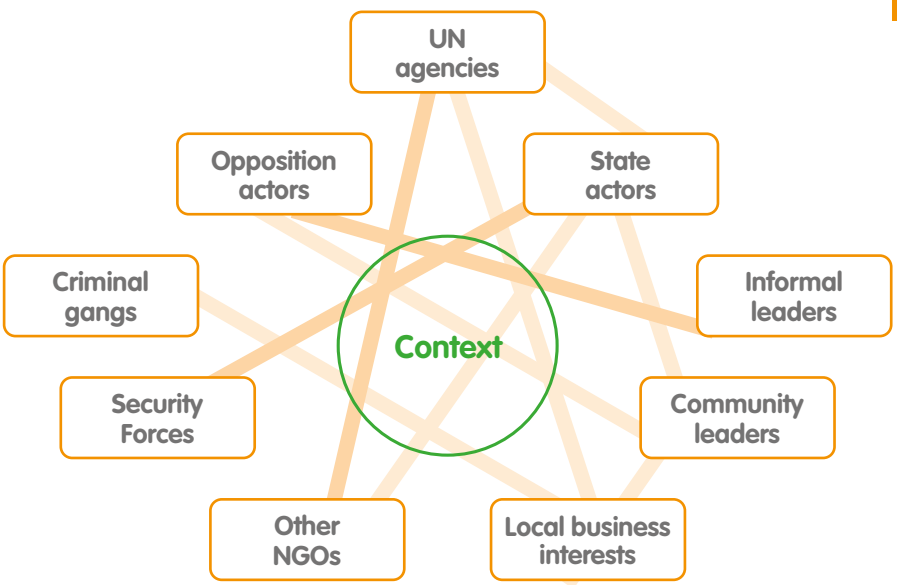
Actor mapping is an exercise to identify all the key individuals, stakeholders or other organisations that will have an effect on the operating environment. They can include:

- Host government ministers, department heads or similar
- Opposition figures, groups or key supporters
- Host government security officials (military, police, other)
- Donors
- UN agencies and their contact points
- Community leaders
- Formal and informal leaders in the operating region
- Other NGOs, both national and international
- Key business individuals who may control local supply and logistics
- Local media
- Beneficiary groups
- Host communities
- Others

Remember, when doing an actor mapping the declared interests of an individual or group may be very different to their actual interests.

Once the key actors are identified, it is important to understand how they link together and where interacting with one may influence relations with another. Think about how they are connected – which actors are allied and which in conflict, for example – as well as how these relationships may be affected by the presence of the organisation and the programmes to be implemented.

Context analysis



The analysis of the context builds on the actor mapping exercise by examining as many factors related to the context as are available. They can include:

- History, both recent and distant
- Cultural and religious traditions that may differ between urban and rural areas
- Racial, tribal or political alliances
- Socio-economic factors
- Infrastructure conditions
- Level of security or insecurity and contributing factors
- Attitudes to foreigners (western, diaspora or regional)
- Attitudes to aid agencies
- Governance issues
- Corruption
- Impact of arriving NGOs, other than programming, on local social, economic and power relationships
- Other factors

In writing a context analysis, you can use the PESTLE format:

Politics

Economics

Social

Technological

Legal

Environmental

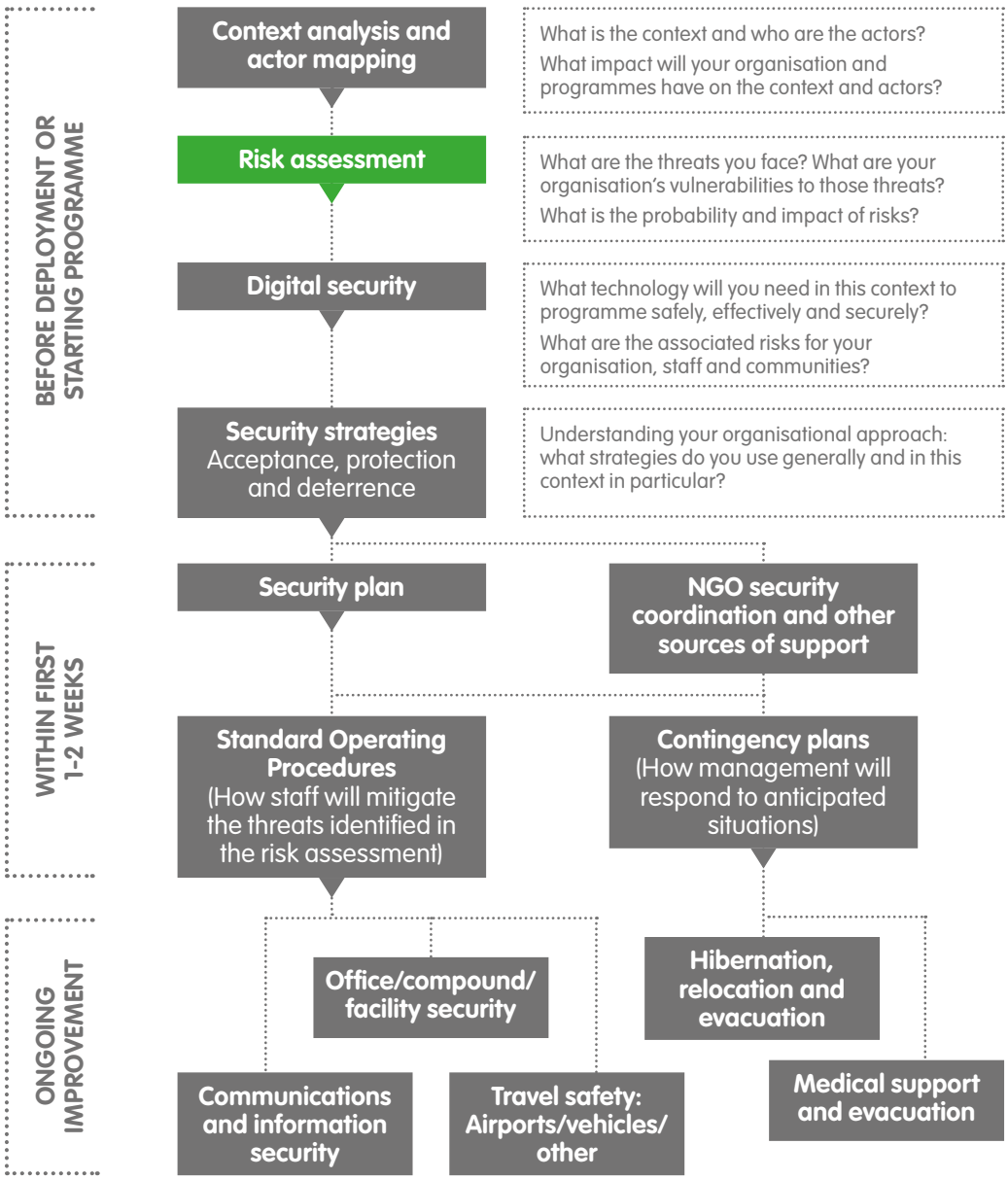
Actor mapping and context analysis may be challenging when responding quickly to a new environment. Identifying all the actors and stakeholders can be difficult enough, without trying to establish power relationships or behind the scenes motivations. It is important to include as many perspectives as possible into the actor mapping and context analysis. Different ethnicities, ages and genders may have distinct understanding of drivers and relationships of the context.

Finding good sources of local knowledge, while being aware of bias, is a good first step, but also research other organisations or individuals who have recently worked in the context and interview them.

In the early stages of a new response, the actor mapping and context analysis should be regularly updated as more information becomes known. The outputs of this process should be maintained as confidentially as possible from a management perspective to avoid upsetting local sensibilities. Also, it is important to not be seen as gathering 'intelligence', so management of the information and how it is employed and shared should be closely monitored.

See Module 9 – Communications and information security

3 Risk assessment tool



It is very difficult to set up safety and security risk management systems if you do not have a clear understanding of the threats or risks you face. Therefore, this should be the first, critical step in any new deployment or programme, once there is, at least, an initial understanding of the context.

The purpose of a security risk assessment is to enable the development of appropriate mitigating measures for implementing safe and sustainable programmes.

The risk assessment process should be done as an integral part of programme and project design. Exposure to risk and mitigation measures are both linked to programme objectives and implementation.

The safety and security risk environment can cover a broad range of threats including violence, conflict, natural hazards, terrorism, health issues, political interference, crime and corruption. This tool is designed to allow organisations or individuals without any specific security background to conduct a basic security risk assessment as part of any wider assessment process.

This assessment tool is broken down into three steps:

Identify the threats → **Evaluate the threats and rate organisation's risk level (vulnerability)** → **Develop strategies to reduce risk and vulnerability**

See Glossary

It is important for all organisations to understand their 'threshold' for acceptable risk as both an organisation and for their staff. Some organisations are experienced and have the capacity to work in moderate to high risk environments while others may only have the capacity to work in low to moderate risk areas. It is important to know the organisation's ability to manage risk when determining the threshold for responding to a humanitarian emergency. The threshold for acceptable risk also depends on the types of programmes being implemented, i.e. whether it is critical for life-saving, advocacy against existing power structures or long term development.

Step 1: Identify the threats

There are many methodologies for identifying threats, including actor mapping and context analysis. However, many of these require a significant amount of research and time in the region and may not be practical in situations of emergency assessment. Nevertheless, organisations should complete at least a preliminary analysis as part of all the initial assessments for project design and implementation. This analysis should be enhanced as more information becomes available.

▶ *See Module 2 – Actor mapping and context analysis*

There are a wide variety of threats and risk that affect international and national organisations entering a new context. Below are some typical ones to consider.

Violent threats

- Targeted armed attack
- Non-targeted armed conflict
- Kidnapping
- Terrorism
- Explosive violence (landmines, IEDs, bombing)
- Carjacking
- Sexual violence
- Civil unrest
- Religious violence
- Crime
- Other?

Organisational threats

- Reputation risk
- Financial risk (banking system, currency exchange, theft, misappropriation)
- Corruption
- Legal risk (work permits, compliance with domestic legislation, resistance to advocacy)
- Political risk
- Workplace violence or discrimination
- Cultural challenges
- Other?

Environmental threats

- Natural hazards (weather, earthquakes, flooding, etc.)
- Medical risks (access to suitable medical treatment for staff)
- Health-related issues (food, water, disease, stress)
- Traffic accidents
- Other accidents
- Fire
- Other?

If the organisation decides to undertake an emergency response programme, a more detailed risk assessment should be conducted within the first 10-15 days of deployment and results incorporated into the overall strategy.

Step 2: Evaluate the threats and rate the risk

Once the organisation has identified the types of threats that it will face, it will need to evaluate each of them and rate the level of risk to the staff, the overall organisation and its operations.

Once each threat is listed and all risk is identified, it is important to rate all risks. This helps clarify how severe (or not) the risk is and how much priority it must be given.

	Threat	Location	Who/what will be at risk?	What will the impact be?
	List the threats identified in step 1 and complete for each of them.	Is the threat confined to one or more areas or across the entire affected region? Be specific.	International staff National staff Community members Marked vehicles Aid supplies	Loss of life Loss of assets Damage to reputation in community/with government Reduction in ability to work
e.g.	Carjacking	Route to airport – Highway 1	All staff Marked vehicles SUV	Loss of assets Reduction in mobility of teams Reduction in ability to work Physical injuries to all staff Loss of life

The risk rating is derived from a combination of the probability that an incident will occur and the level of impact it will cause.

Most NGOs and the United Nations use a risk rating system similar to the following:

1. **Very low**
2. **Low**
3. **Medium**
4. **High**
5. **Very high**

Threats may vary in level geographically. It may be necessary to evaluate the risk by locality rather than nationally or regionally. For instance a border area may have a likely probability of armed conflict while in provinces closer to the capital this may be unlikely. Depending on the scale of the emergency situation you may have one overall risk rating for the area or several within the affected zone for each type of risk.

Threats may also vary due to different levels of staff vulnerabilities. For example, sometimes national staff may be at less risk in a specific area than international staff. Ethnicity, gender and experience can also affect the vulnerability of staff.

Below is a table you can use to determine the risk rating for each threat that has been identified. Where possible use previously reported incidents of various types of threats to justify the risk rating level assigned. However, in a new situation where humanitarian responses have not recently been undertaken it may be necessary to use data from similar interventions combined with current information from local sources. The definitions for each level should be agreed across the organisation to make it possible to compare different contexts.

Impact	Negligible	Minor	Moderate	Severe	Critical
	• No serious injuries • Minimal loss or damage to assets • No delays to programmes	• Minor injuries • Some loss or damage to assets • Some delays to programmes	• Non life-threatening injury • High stress • Loss or damage to assets • Some programme delays and disruptions	• Serious injury • Major destruction of assets • Severe disruption to programmes	• Death or severe injury • Complete destruction or total loss of assets • Loss of programmes and projects
Probability					
Very unlikely Every 4+ years	Very low	Very low	Very low	Low	Low
Unlikely Every 2-3 years	Very low	Low	Low	Medium	Medium
Moderately likely Every year	Very low	Low	Medium	High	High
Likely Once per week	Low	Medium	High	High	Very high
Very likely Daily	Low	Medium	High	Very high	Very high

Some organisations may have a security level system that is developed based on the overall level of risk to the organisation, programmes and staff considering all of the different threats. The development of a security level system is not covered in this tool.

Step 3: Develop strategies to reduce risk and vulnerability

Once the threats that may affect a humanitarian response have been identified and evaluated, and the risks rated, it is important to recommend risk mitigation measures to address these vulnerabilities. While no two situations are identical, there are normally actions that can be followed to reduce exposure to risk.

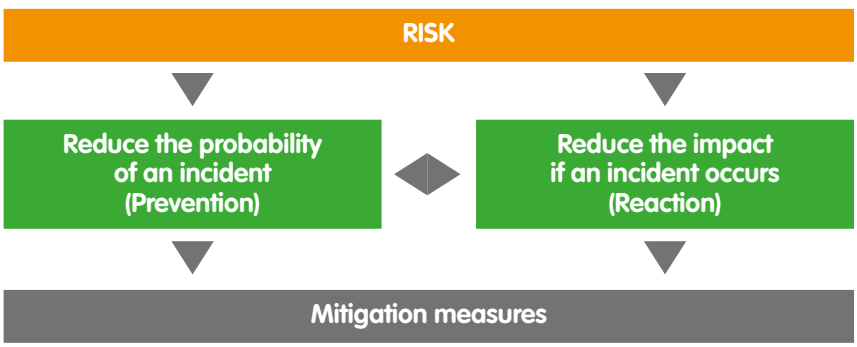
Developing security strategies is a critical step in ensuring that before committing staff, resources and the organisation's reputation to a response, the agency has taken all reasonable steps to minimise the risk.

This is an essential component of the duty of care. Mitigation strategies should reflect the organisation's preferred risk management strategies, such as acceptance, protection or deterrence.

▶ *See Glossary*

▶ *See Module 5 – Security strategies: acceptance, protection and deterrence*

In general, reducing exposure to risk takes two forms:



Measures to reduce risk should focus on both prevention (reduce the probability) and reaction (reduce the impact). By doing this you can reduce the level of residual risk from the level originally assigned to each threat identified and thereby improve your ability to deliver emergency response programmes. It is important to remember that the goal of security risk management is not to put up barriers to delivering programmes but to enable organisations to stay engaged and able to implement projects despite the level of risk.

For example, we could reduce the exposure to the risk of vehicle accidents by:

Reduce probability

- Ensure vehicles are well maintained
- Enforce speed limits
- Provide driver training
- Avoid travel after dark outside towns
- Avoid congested high risk routes
- Avoid travel in extreme weather

Reduce impact

- Ensure seatbelts are always worn
- Have first aid kits and train staff
- Have a fire extinguisher
- Keep emergency contact numbers
- Place safety warning triangles
- Have insurance and counselling

Some threats like office fire, thefts or vehicle accidents can be reduced through good prevention strategies. However, threats such as natural disasters, infrastructure failure or political risk will be largely unpreventable, so the focus will be on reaction to reduce the impact on staff and programmes.

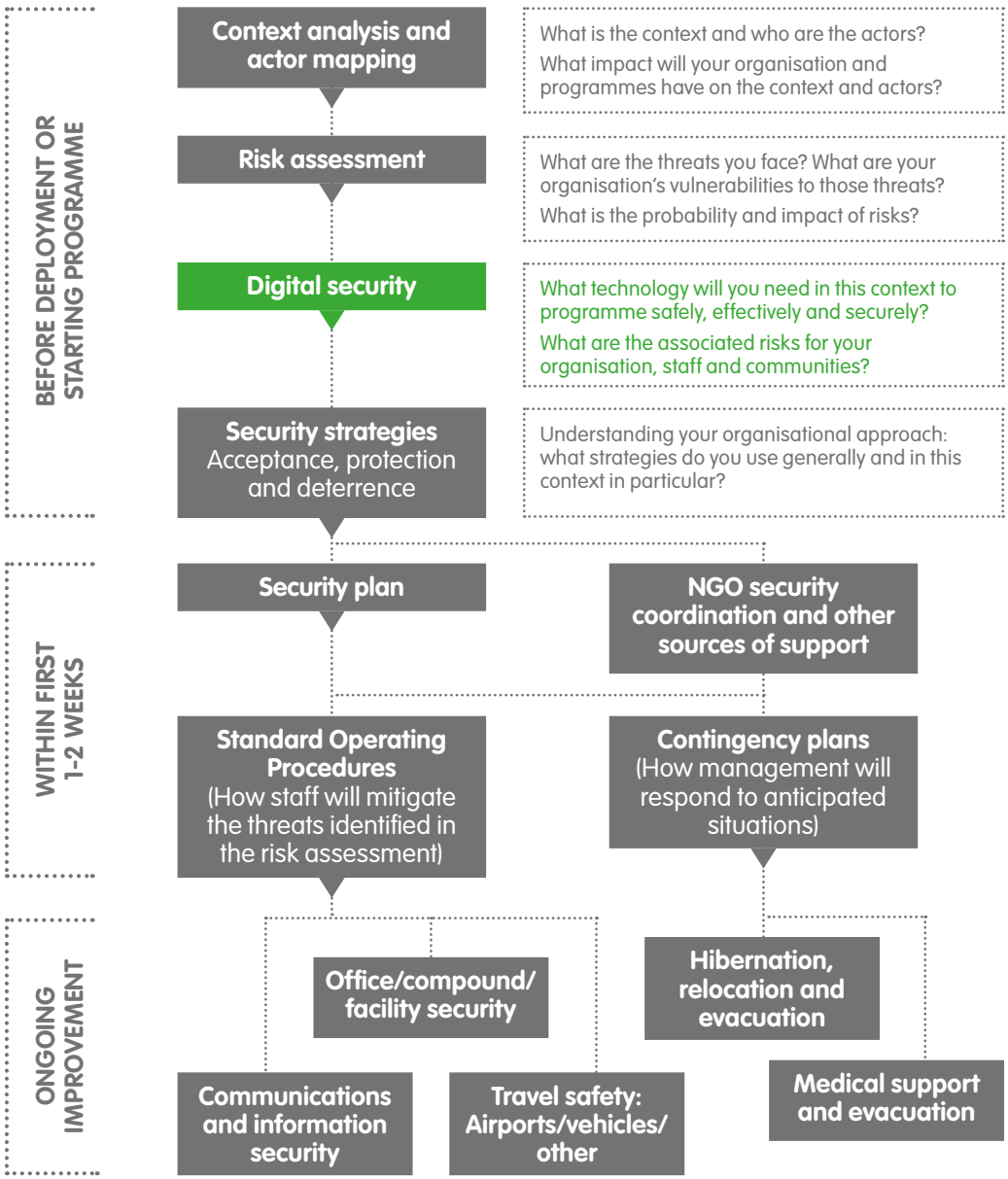
When possible, identify reliable early warning systems that can assist your organisation in mitigating the risk. Some reaction measures can be put in place as part of organisational preparedness, such as provision of first aid kits, first aid training, stockpiling emergency supplies or personal security training.

Mitigating measures should reflect the risk assessment. For example if a particular threat is identified as being very unlikely but with critical impact, implementing measures only to reduce the probability will have limited effect on reducing the risk.

Increasingly, many organisations are choosing to work through local partners as a means of reducing their exposure to risk, especially in challenging contexts. However, this will transfer risks onto the local partners. Although the overall threat to the local NGO will remain the same it is important to understand that the resultant risks can be very different, and just because the partner organisation is local, it does not mean they will have no exposure to risk.

▶ *See EISF paper 'International agencies working with local partners'*

4 Digital Security



In the modern world, technology has become so entwined with our lives that we rarely pause to consider its implications. It becomes difficult to imagine life without our devices, and even more challenging to consider our work without associated software and apps, video calling, the cloud, emails, servers and the various accounts that help us to connect with our activities, colleagues and relatives. If technology is a powerful enabler, it is crucial to consider how this ever-present fact of life can put ourselves, our organisations, and our work, at risk.

This module provides basic advice for NGOs to integrate digital security within their overall security risk management processes.

Digital Security: The measures, strategies and processes that aim to mitigate risks related to organisations' and individuals' digital footprints and use of technologies.

Given the rapid pace at which technology evolves, some of the measures included in this module will need to be reviewed against up-to-date advice from reliable sources. There are many organisations that can provide digital security support and help you to build your policies. Among others, you can refer to the Frontline Defenders Digital Security & Privacy Handbook, the Digital First Aid Kit, the UK National Cyber Security Centre, Access Now, Security Without Borders and the Umbrella App.

Context analysis

To fulfil duty of care obligations and protect staff from physical and psychological harm, organisations must mitigate risks related to their digital presence and activities. When NGOs are starting a new project or entering a new region, both context analyses and risk assessments should therefore include digital security vulnerabilities.

When conducting a context analysis, consider exploring some of the following elements:

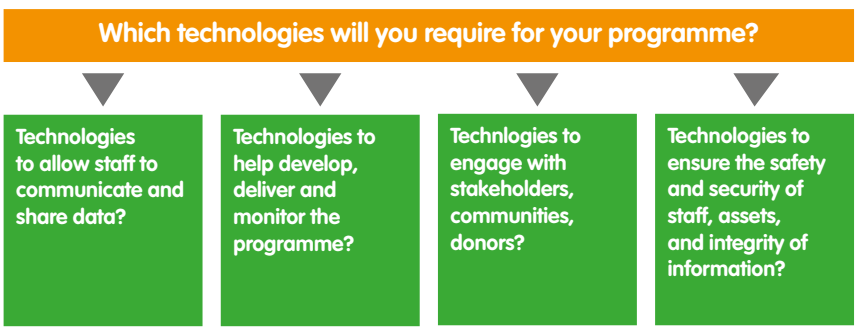
The legal context	**International/regional level** – For European-based organisations, data protection regulations such as the EU *General Data Protection Regulation* (GDPR) must be considered. They will affect how you collect, use and store data on individuals. It is also important to verify whether a Data Protection Impact Assessment (DPIA) is required for the data you are working with. **Country level** – Many nations are setting increased legal controls on technology. In several contexts, the use of equipment like radios and satellite phones are strictly controlled and may even be illegal. In other contexts, the use of encryption, as well as certain websites and social media, is prohibited.

The political context	**Government monitoring** - In areas where NGO support for the civil population is needed, the host government may be not only suspicious, but actively engaged in overt and covert monitoring of NGOs' activities, reports and communications. As well as this, home and donor governments increasingly require access to, and oversight of, the data handled by NGOs. Such involvement may carry serious implications for your programmes. While NGOs must adhere to the principle of transparency, we often possess information (on staff, beneficiaries and programmes) that is confidential in nature. **Network shutdowns** – Several governments have extensive control over communication networks and, in times of civil unrest, may declare internet shutdowns. Given NGOs' increasing dependence on technologies to operate, it is essential to consider this possibility and develop adequate plans to sustain communication channels.
The cyber crime context	This is often the most challenging area for NGOs. Not only do organisations need to assess locally-specific cyber risks, but they also need to be aware of the global cyber crime environment. Attacks on computers or mobile phones can be launched remotely and must be considered during travel.

Technology Needs Assessment

Every type of programme attracts different risks. Emergency response programmes may be more sensitive to blackmail, fraud or safeguarding threats. Advocacy and human rights campaigns may be targeted by various groups, seeking to damage the organisation, or to collect personal information on beneficiaries and staff. Development projects are also vulnerable to the diversion of resources and corruption. Even internally, NGOs use a range of technologies for their various operations, from communications to data gathering to implementation monitoring.

In order to accurately assess the threats that you may face and develop risk mitigation strategies, the first step is to identify what technology will be used. For this, you need to thoroughly understand your programme and consider the digital actions of the different stakeholders involved, such as staff, communities, donors and host governments.



Many NGOs are reluctant to explore new technologies due to the initial efforts required to train their staff and adapt their processes. However, when wisely incorporated into our activities, innovation can make programming both safer and more effective in the long term.

Technologies regularly used by NGO staff		
Equipment	**Communication devices**	**Software and apps**
Laptops/desktops/tablets External storage devices GPS/navigation systems Batteries/power-banks Vehicle tracking systems Scanners/printers Wireless devices	Smartphones/mobile phones Landline phones Satellite phones Radios/radio repeaters	Cloud-based file sharing Shared data servers WhatsApp and other messaging apps Skype and other video calling software Email Social media

Digital Risk Assessment

Understanding the digital risks that your staff, organisation and programmes face is a complex and difficult task – especially considering that cyber threats continually evolve. Many security advisers delegate this function to their organisation's Information Technology (IT) department, or to a trained member of staff. However, many digital incidents are not due to technical flaws, but rather due to 'digital misconduct' among staff. Improving an organisation's digital security, therefore, requires developing standard operating procedures (SOPs) and effective policies to guide staff in their use of technology.

Every staff member has a critical role to play in digital security!

Typical Digital Threats

Nowadays there are a wide variety of digital threats, which can affect both the organisation and its staff:

Organisation
• Hacking of files • Reputational damage, defamation • Communications monitoring or spying • Damage caused by viruses • Theft of devices • Fraud/financial theft • Misinformation/fake news • Theft of data pertaining to staff or beneficiaries

Staff
• Scamming, blackmailing • Movement tracking, targeting • Technology-induced stress • Fraud/financial theft • Misinformation/fake news • Theft of personal data • Identity theft

Online threats usually come in one of two forms:

- **Direct Attacks:** Attacks aimed at an individual or organisation's system for a specific purpose.

  Examples include: brute force (computer programmes attempting to break into a target computer by guessing possible combinations of a target's password), key loggers (virus softwares that identify passwords), proximity (direct surveillance).

- **Indirect Attacks:** Attacks of broad spectrum that often take the form of scams or phishing attempts, which may not be directly aimed at your NGO/staff.

  Examples include: phishing (fraudulent emails disguised as those from a trustworthy entity, which ask the recipient to perform certain actions such as clicking links or opening attachments).

Direct and indirect attacks can also be seen in social media environments, targeting either individuals' or organisations' accounts.

Don't forget to consider staff's diverse profiles when assessing threats. It is an organisation's responsibility to inform staff of the risks associated with the use of certain apps and technologies.

Particularly in countries where LGBTQ+ rights are not respected, staff can face serious threats from the use of specific dating apps (for example, being 'outed' online, blackmailing and physical assaults).

▶ *For further information, see EISF paper 'Managing the Security of Aid Workers with Diverse Profiles'.*

Digital Security Strategies

With your digital risk assessment complete, you should develop clear strategies to mitigate the identified risks. In recent years, staff misconduct and abuse scandals, combined with a rise in suspicion and political accusations, have placed NGOs in difficult positions and caused damage to their reputations. In addition,technological progress and the rise of social media has created a space where misconceptions and rumours can spread quickly, making NGOs ever-more vulnerable to reputational threats.

Given the importance of public perceptions and community acceptance for NGOs' access to populations in need, developing a clear digital security strategy is key for an operation's success. This document should fit within the general security policy and align with the organisation's approach to duty of care and security risk management.

The digital security strategy should cover three basic components:

Organisational Security	Staff Security	Community Security
• Internal network security (how will you establish a secure intranet, control access and protect data?) • If your NGO already has an internal network system in place, what confidential or sensitive information will this platform be collecting? • Acceptance/ reputational risk (how will you monitor and respond to negative accusations online?)	• How will you protect staff data (payroll and HR records, contact information, data stored on work devices)? • How will you maintain communications - especially in emergencies? • How will you support staff targeted by digital attacks? Do these measures protect staff with a diversity of profiles?	• How will you manage programme information to comply with 'do no harm' and safeguarding imperatives? • How will you comply with data protection regulations such as GDPR? • Can your existing feedback mechanisms and complaint response systems address online/social media abuse?

The digital security of staff, the organisation and the community is overlapping. Because a breach in one area will have repercussions for the others, it is important to consider their interdependence to devise a consistent and comprehensive approach to digital security.

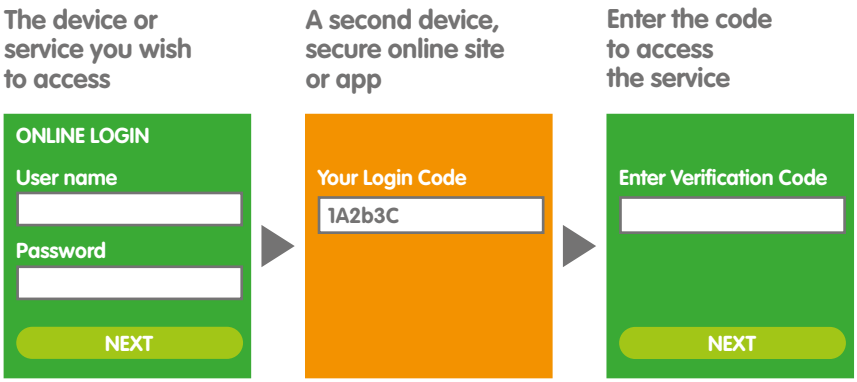
An inclusive strategy should take into account the specific risks faced by local staff and partners. In many instances, they are exposed to greater, and longer-term, repercussions from local governments and communities.

▶ *See GISF research paper 'Partnerships and Security Risk Management: From the local partner's perspective'*

Digital security policies should provide clear guidance on what is or is not allowed within the digital environment. They should cover the following points:

1. **Internal platform and devices:** Staff access and exit procedures, including the deletion of personal data, password protection mechanisms, anti-virus software/firewalls, protocols for data back-ups, software update regulations.

One mitigation measure is adding two-factor identification to all of your devices and key online services. This a valuable added security measure to prevent unauthorised access to your systems and devices.



2. **Information security:** Confidentiality policy and classification system - e.g. confidential, restricted, internal or suitable for public use, legally-compliant information sharing regulations.

Information security documents often refer to the three AIC principles:
1 availability (guarantee of access to information),
2. integrity (assurance that information is reliable) and
3. confidentiality (control of access to information).

See Module 9 - Communications and Information Security

3. **Communications:** Encryption regulations, audio-communications protocols, use of apps for work-related communications, log retention procedures.

Advise all staff to be cautious when following links in emails. Never open attachments in suspicious messages and beware of obscure file types such as .exe, .ink, .jar, .dmg, .wsf and .scr. Watch out for misspelled names and addresses – instead of 'a.person@your-ngo.org', a fraudulent address may read 'a.person@your-ngo.net'.

4. **Travel and network access:** Guidelines on the use of Virtual Private Networks (VPNs) or public or insecure networks, guidance and regulations on device protection).

Travel and network access policies are especially important for areas where governments and officials are suspicious of NGO activities, as there may be a heightened risk of monitoring and/or data theft.

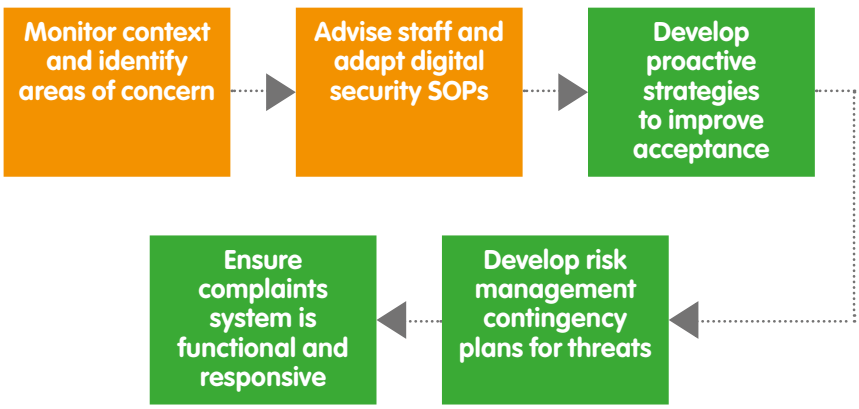
While wiping information from laptops, phones and other devices before travel may seem like a good security measure, this level of precaution can actually risk raising suspicion. When travelling, it is therefore preferable to keep only necessary, non-confidential information and avoid having devices too 'clean'. Consider using secure deletion tools such as CCleaner and Eraser. Doing regular back-ups of important files also prevents having your files ransomed.

5. **Social media:** Guidelines on posting sensitive information which align with the code of conduct, rules on the delay required when posting locations of travel (including geotagging), systems for reporting abuse and attacks against staff or the organisation).

Incorporating Digital Risk Management into Security Plans

Building on their existing security risk management policy, an office or programme team can develop a digital security plan that suits their current context and operational needs. Digital security challenges should feature as a component of the overall security plan to advise staff on the necessary risk mitigation procedures.

Constant monitoring of the local context and digital security environment is critical to the success of your programmes and the safety of your staff.



Training staff on digital security measures and regularly updating them on new and emerging threats is key. As technology-based risks evolve, we must ensure that staff are aware of the various threats that exist (for instance, malwares that can record audio, activate webcams, take screenshots and alter files) and that they adopt sound behaviours to mitigate associated risks.

Training should be adapted to the digital culture and competency of its public. In many regions, downloading pirated or copied softwares to work devices is common practice. Staff's social media habits and preferred communication apps (Whatsapp, Telegram, etc.) will also generate different risks – both to themselves and to the organisation.

HTTP versus HTTPS

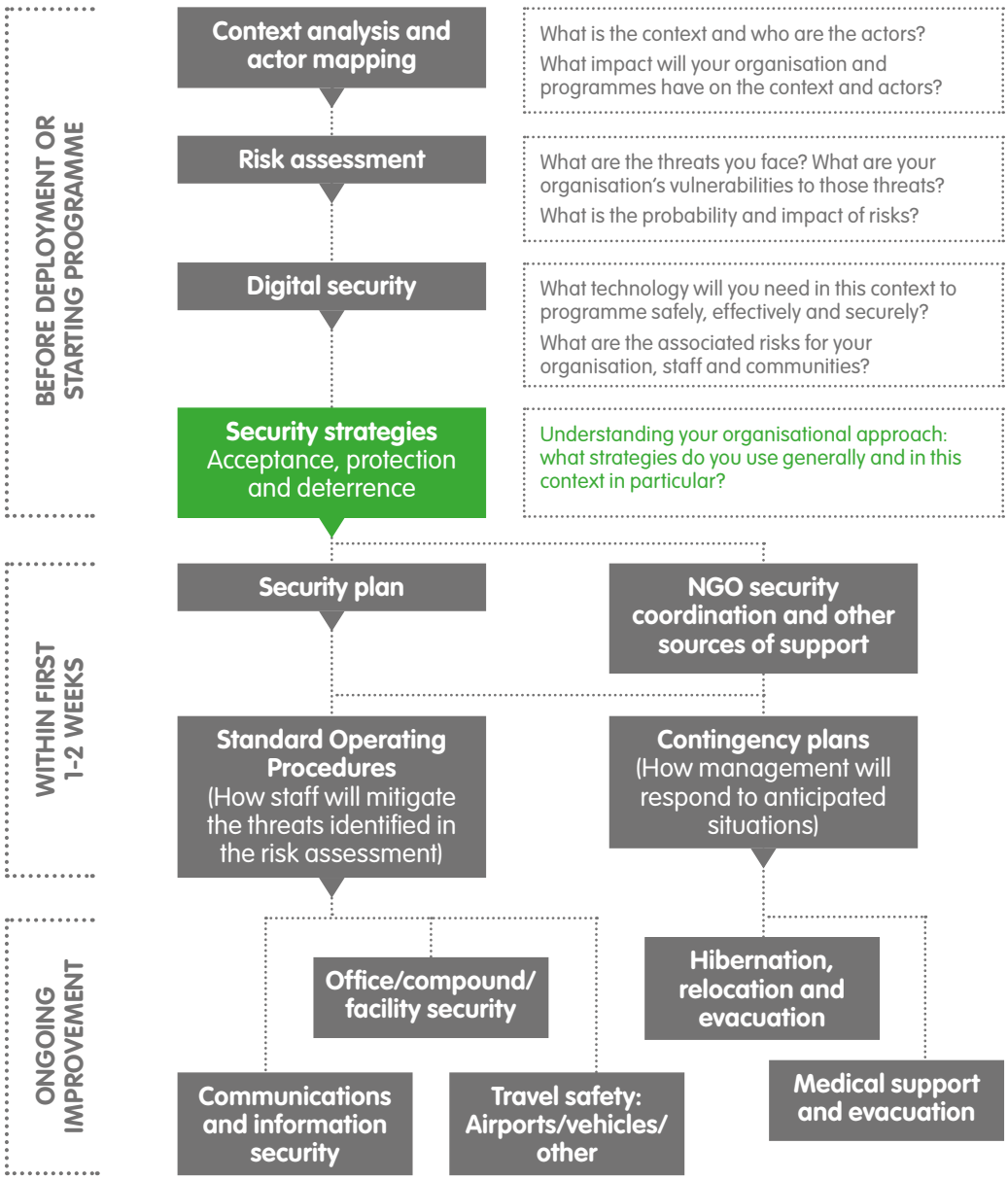
All websites are identified by a Hyper Text Transfer Protocol (HTTP) leader in an online address. Websites that are verified as secure feature an HTTPS leader in the address line. Many modern browsers will provide a warning if you try to connect to a non-secure HTTP web address, or will block access entirely. Staff should be strongly advised against visiting insecure websites.

Below are examples of digital security measures that can be included in **Standing Operating Procedures** (SOPs). Note that these SOPs will need to be adapted to the relevant context analysis and risk assessment, as well as the wider programme and organisation.

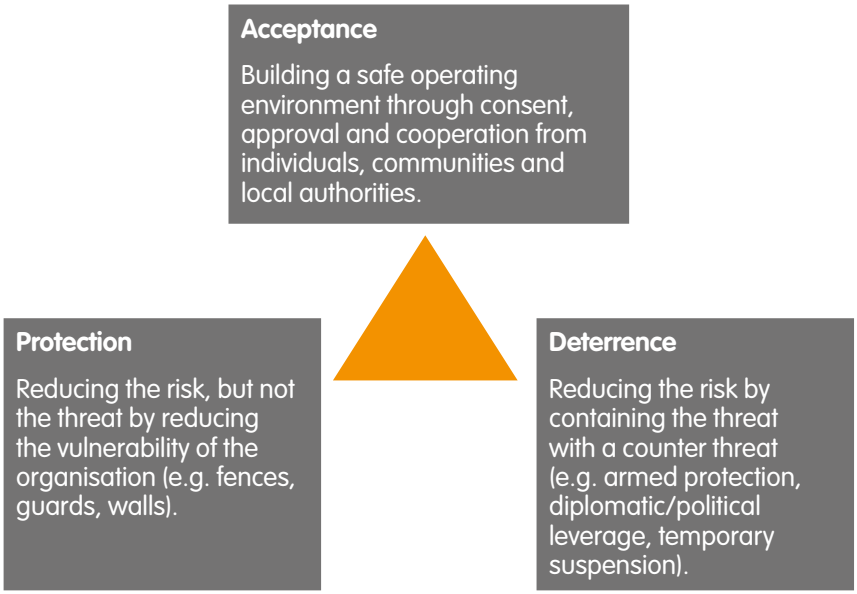
Staff Network Access	• Staff can access the server only once they have completed a full HR induction. • Login must be completed only through the office server or the organisation's virtual private network (VPN). • Passwords should contain a combination of upper and lower case letters, numbers and special characters, and avoid using words that can be found in the dictionary. For example, *M*d0gH@zF!ea5* (my dog has fleas). • Do not record nor share your passwords and don't allow websites or browsers to store them. Instead use [insert organisation's preferred password management tool].
Data and information security	• All data contained on staff devices and server drives are considered confidential, including beneficiary data. • The release of any data outside of the organisation, including with specific donors and media must be approved by [insert relevant person]. • Conform to the confidentiality policy and use encryption for highly confidential communications for example, [insert organisation's preferred app] for mobile messaging.

Software and passwords	• All software and apps installed on devices provided by the organisation must be approved by [insert relevant person]. • Staff must install software updates immediately when notified. • Staff must not use the same password for multiple accounts, whether personal or work-related. • Staff must report all suspicious emails to [insert relevant person] and must never download attachments unless the sender is confirmed. • All devices must have privacy screens that auto-lock after a maximum of 3 minutes of non-use.
Staff travel	• Staff are responsible for ensuring that they have effective communications systems when travelling outside of main urban areas, and can recall their emergency numbers from memory. • When travelling to [insert relevant risk rating] areas, staff are advised to back up all personal and work files prior to travel. • Staff must not operate any devices while driving a vehicle.
Social Media	• Staff should not post any information online that is related to their work or travel plans, including via private social media accounts. • Stories or images gathered on the trip may be sent to [insert relevant person] for review and possible use by the organisation. • Staff must conform to the code of conduct in their personal social media activity at all times. • Staff should record abuses and report any online bullying or negative stories related to the organisation or its programmes to [insert relevant person].

5 Security strategies: acceptance, protection and deterrence



There are typically three security strategies used by humanitarian aid organisations in all contexts.



Generally, international and national aid organisations prioritise the acceptance strategy as their preferred approach. However, this can take time and organisations deploying to new areas cannot just assume they will have the acceptance of the community. An organisation may focus initially on protection and deterrence measures until acceptance has been developed. However it is important to note that behaviours from day one will impact future efforts to develop acceptance.

Acceptance

After a rapid onset emergency it is challenging for host governments and communities to distinguish between different organisations when a flood of new international and national NGOs, and United Nations agencies arrives in the area. This can be complicated by rapid turnover of staff in the first few weeks as first responders hand over to longer-term staff. All staff deployed and local employees – including managers, community mobilisers and drivers – should be briefed on how your organisation will employ the three strategies and how acceptance will be built with all stakeholders.

Building acceptance is not only about the communities an organisation works with, but about all its stakeholders. An actor mapping will help the organisation identify which stakeholders may be affected by its programmes and what allies it may have in developing acceptance with them. Remember that what an organisation and its employees say locally is not the only means stakeholders can get information. Many communities now have access to the internet, so the messages communicated must be consistent with what is on your website and social media accounts.

Acceptance has to be earned and can be lost very easily, and the behaviour of one responder can affect the whole community. Acceptance must be approached proactively.

Key points:

- Be clear about who you are, your agency's background and priorities, where your funding comes from and how your programmes are developed.
- If you are a faith-based or secular organisation, be clear about how this does or does not affect your work, especially in a strong religious environment. Also be aware of how you will be perceived.
- Understand who your partners are, how they are perceived and what impact your relationship will have on their, and your own, acceptance.
- Ensure stakeholders are engaged before commencing any work.
- Have a rigorous complaints system and be seen to follow up on concerns.
- Do not isolate your staff from communities. Stay visible and accessible.

Protection

Protection measures should be developed in line with the risk assessment, and it should be ensured that they are applied equally across all staff (local and international), and seniority levels. Organisations should provide training in security measures to staff, give orientations to new employees, and pursue coordination with other agencies or security forums.

▶ *See Module 6 – NGO security coordination and other sources of support*

The physical protection of buildings, compounds and/or distributing sites should not make it appear that the organisation is building a bunker or a fort. Compounds and other office or working space should blend in with the buildings in the vicinity.

▶ *See Module 8 – Security of facilities*

It is important to focus on the best communications systems the organisation can afford, or that are available, including radio, internet, mobile, landline, satellite, fax, informal couriers or other. Communications systems should be accompanied by policies for staff reporting in (regularly or on a schedule) to ensure safety.

See Module 9 – Communications and information security

Deterrence

Deterrence is usually the last resort strategy. It is used when acceptance and protection have not been successful or have proven inadequate. In some contexts, it may also be required by host governments (e.g. Somalia, Chad, Niger).

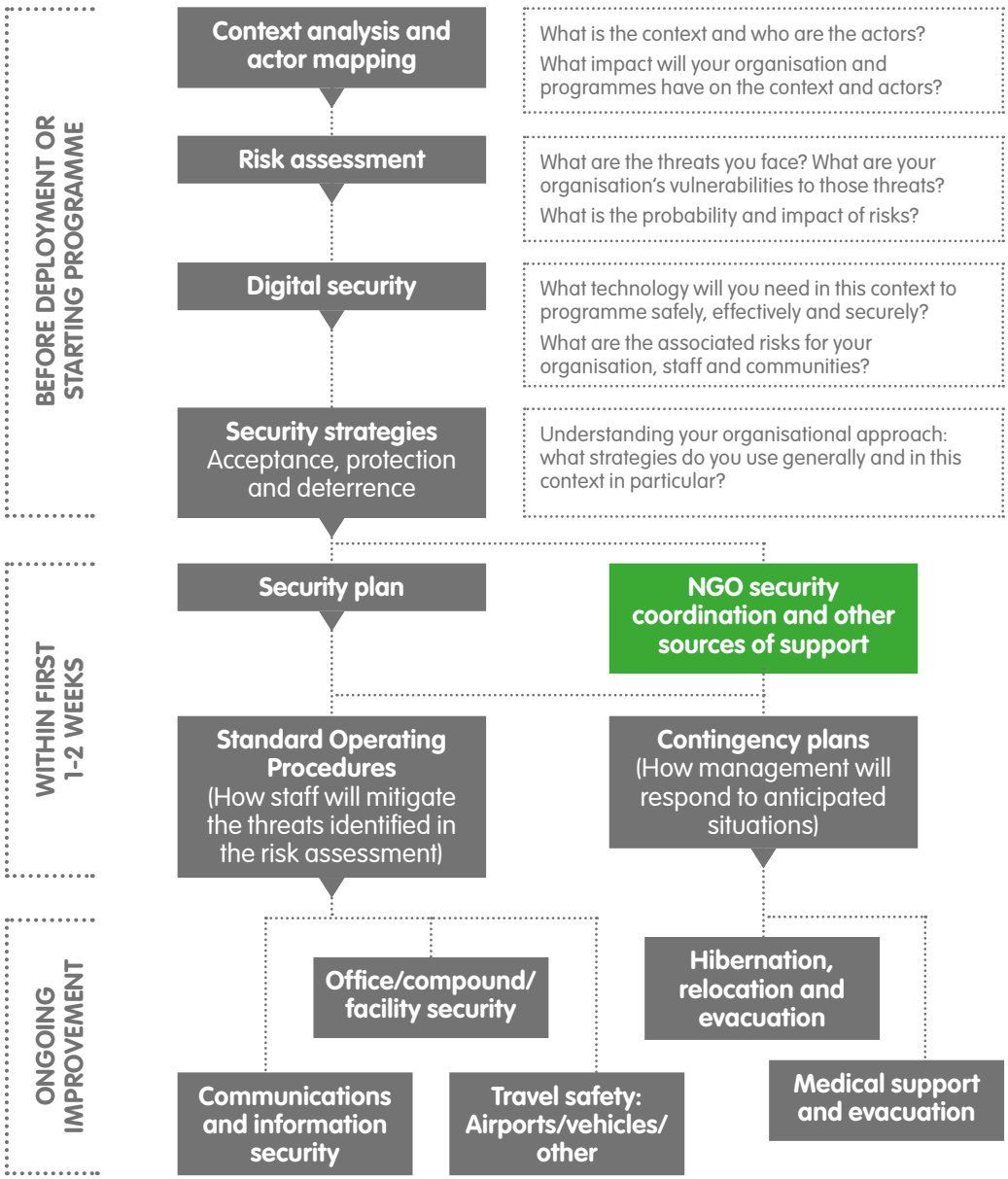
Withdrawal of services is the main threat that can be used in an insecure area but the organisation must ensure first that local governments and donor agreements are not compromised. Do not make empty threats.

Armed guards or military and police escort should be avoided where possible as they will often make acceptance impossible or very difficult – even at a later stage. They may also increase the risk of injuries from crossfire, or the risk of extortion or harassment.

See EISF briefing paper 'Engaging private security providers: a guideline for non-governmental organisations'

When considering the different security strategies it is important to understand the mission, vision and mandate of the organisation. All organisations are different in not only their mission and programmes, but also in their vulnerabilities and capacity to respond to them. Just because one organisation is implementing a particular strategy does not mean it will work for another agency, even if they are working in the same context.

6 NGO security coordination and other sources of support



In any country where aid organisations congregate in response to an emergency or ongoing crisis, various forums and coordination groups often develop. In regions where insecurity is an issue, NGO security-dedicated forums may also form. These may be part of a broader NGO coordination body, a stand-alone body or an informal group for information sharing and coordination.

Security forums are usually chaired by one organisation and attended by security focal points of the member organisations. These forums generally share context assessments and reports on incidents. They may also share the costs of organising training for staff, advise on recommendations from embassies or host governments, and can act as a central coordination point with other actors such as UNDSS. If a forum is available it is strongly advised that organisations join, both to gather context information and to identify best practices for that particular country.

Membership of a security forum is not a substitute for an organisation completing its own risk assessment and developing working relationships with key actors such as UNDSS or other agencies.

When appointing a staff member to attend these coordination meetings, ensure they are supported in dedicating time to this as a priority as well as being fully briefed on the rules for participation – in particular, how the information shared is to be managed. Ensure they are supported in sharing outputs within the organisation to maximise the benefit of the membership to the coordinating body.

There are a number of sources of additional information that organisations can link into to improve the flow of information on incidents, find advice on how to mitigate risks from various threats and improve security capacity. For instance, 'Saving Lives Together' (SLT), is a framework for security collaboration between NGOs and the United Nations. It comprises a set of recommendations such as sharing information and resources, based on best practices in security risk management. While the United Nations does not take responsibility for evacuation, communications, and other support services, they may coordinate such services in certain contexts.

The latest version of the SLT framework was released in 2015 and is accompanied by guidelines on expectations regarding the NGO-UN collaboration. SLT is not the exclusive domain of UNDSS, but the latter is the lead agency within the United Nations system. Local contacts for UNDSS can be identified through HQ members of the SLT – such as EISF or InterAction.

Other sources of safety and security information are:

- National governments, including donor governments and their embassies.
- Host government departments.
- The European Commission's Humanitarian Aid and Civil Protection Department (ECHO) which produces security material for aid organisations in some contexts.
- Insurance providers, as they will often have a threat advisory service linked to various countries and/or regions.
- NGO security consultants.
- Local commercial security providers (guard companies).
- International and national media.
- Other NGOs and their partner organisations.
- Host and beneficiary communities.
- National staff.
- Insecurity Insight.
- Aid Worker Security Database.
- International NGO Safety Organisation (INSO) if available.
- European Interagency Security Forum (EISF).

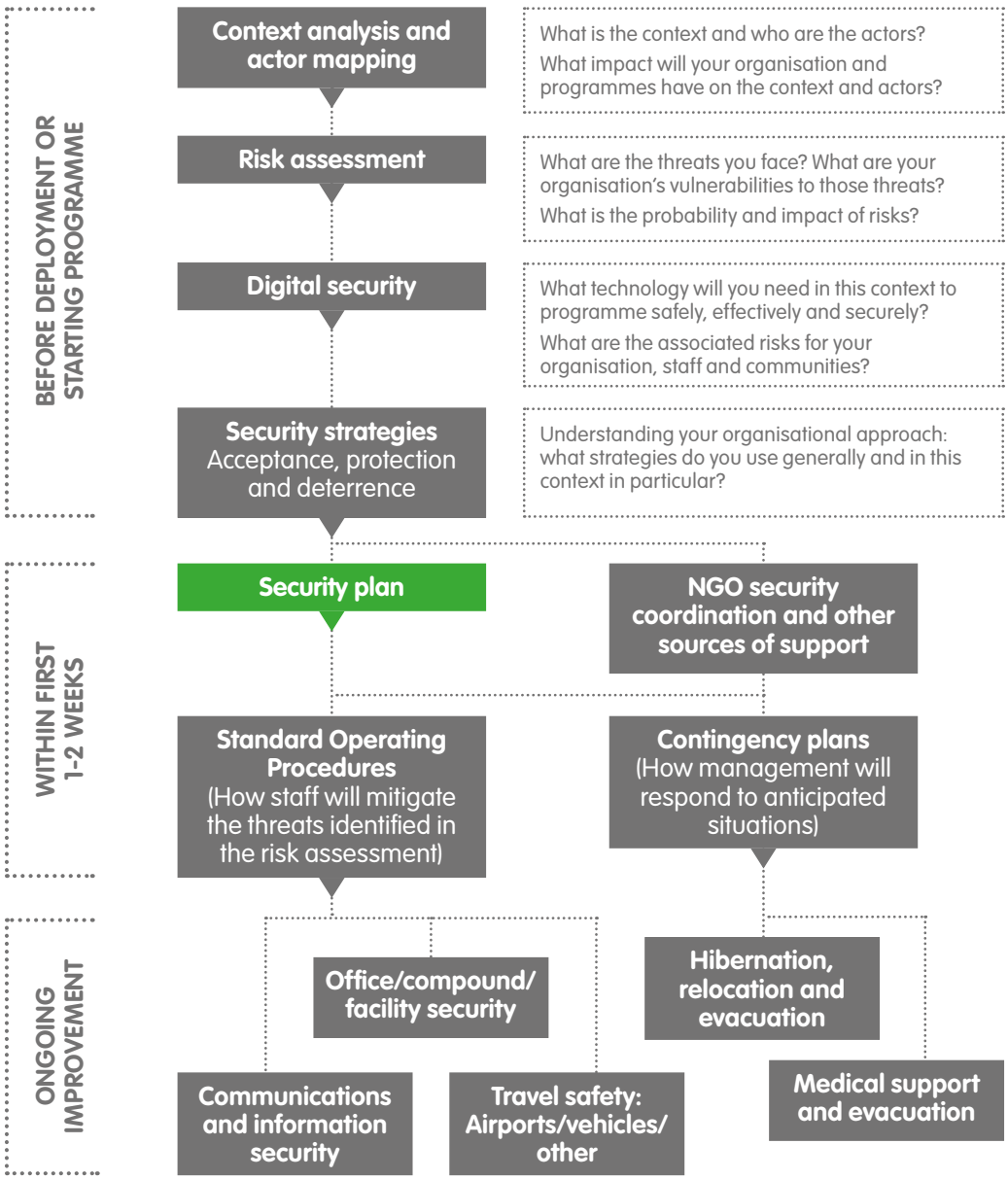
Making good decisions requires reliable and accurate information. All information must be considered against the reliability of the source, the number of separate individuals/organisations reporting the same information, and any local bias. Generally, avoid acting on rumours without confirmation by a reliable source.

▶ *See Module 9 – Communications and information security*

In an emergency or crisis situation, the safety of staff, your organisation and possibly also beneficiary communities will depend on your ability to take decisions and activate contingency plans. There are a number of systems for rating the quality of information. Below is a simple grid to help in assessing information received.

	Detailed and credible information	Vague or incomplete information
Trusted, reliable source	**Good information for decision-making**	**Consider information and seek confirmation**
Unknown or unreliable source	**Seek confirmation from known source**	**Do not disregard but do not make decisions without another source**

7 Security plan



Security plans are not strategic documents. They must be simple, easy to use and provide information in a format that staff can use in their daily work; otherwise the document will not be read fully or utilised. To be manageable, security plans should be no longer than 20 pages or staff will not read, remember or make use of the document.

There are many variations on security plans. However most follow a general format and contain similar sorts of information depending on the organisation, the type of engagement, number of staff and size of assets, location of projects, operating context and other localised factors.

Security plans are best created by a mix of staff including senior management, administration, programme management, field staff and drivers as well as a mix of different nationalities, ethnicities and genders. Each will offer a different perspective.

By using a mix of staff, national and international, country office and field staff you can create a sense of ownership of the plan and improve compliance. However, avoid having too much of a management focus as front-end staff in the field may be most at risk. Similarly, avoid excessive focus on international staff, and consider the exposure to risk for all staff, e.g. also national staff delivering programmes. If the security plan includes different measures for international, national-relocated and local staff, the reasons for this should be explained clearly to all staff. Otherwise the organisation may be perceived as only caring for a particular group within the staff.

The security plan, or at least the relevant parts, must be available in the language of the users. For non-literate staff, and if translation is not feasible, consider how the information within the security plan will be disseminated. It is important to include and explain the security plan to all staff based in the office, including cleaners and watchmen. Staff members that are not as involved in the organisation as programming or management staff can be more vulnerable to offers of money for information. They know less about the mission of the agency and may have less interest in ensuring the safety of all staff.

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

You can use the template below to ensure that your security plan has all the main elements.

I. Overview of security plan

- Purpose of the document

Why is this document important for all staff?

- Who is responsible for preparing the plan, updating it and training staff?
- Your risk threshold

What level of risk can your organisation manage? What is too much?

- Your security strategy

How does your organisation utilise acceptance, deterrence and protection strategies? How do you evaluate the results?

▶ *See Module 5 – Security strategies: acceptance, deterrence and protection*

- Date of document/update/reviews

When was the document written? When should it be updated?

II. Current context – your risk assessment

▶ *See Module 3 – Risk assessment tool*

- The overall context

A good, general description of the country and the region, and the challenges faced.

- Your risk assessments system

How are you identifying threats and your system rating?

- Threats you face in your context
- Evaluation of threats and rating of risk

III. Standard Operating Procedures (SOPs)

This section should include SOPs for all the threats and risks identified in your risk assessment. They must be simple, clear instructions for how staff should prevent risk (reduce probability) and/or how to react if an incident occurs (reduce impact). It should be in the format of checklists, procedures or actions.

- Cash in transit
- Communications, including social media plan

▶ *See Module 3 – Risk assessment tool*

- Incident reporting
- Field travel and vehicle safety

▶ *See Module 10 – Travel safety: airports, vehicles and other means of transport*

- Fire in office or compound
- Office and facility access control
- Robbery
- Vehicle accident
- Include other SOPs

IV. Other key sections

- Health and safety

Staff protection from health threats (malaria, HIV, etc.) as well as accidents, stress, post traumatic stress disorder (PTSD).

- Human resources

Policies related to recruitment, background checks, contracts, confidentiality, etc.

- Administrative and financial security

Policies for preventing theft, fraud, corruption as well as cash handling and procurement.

- Include other key sections

V. Crisis management section

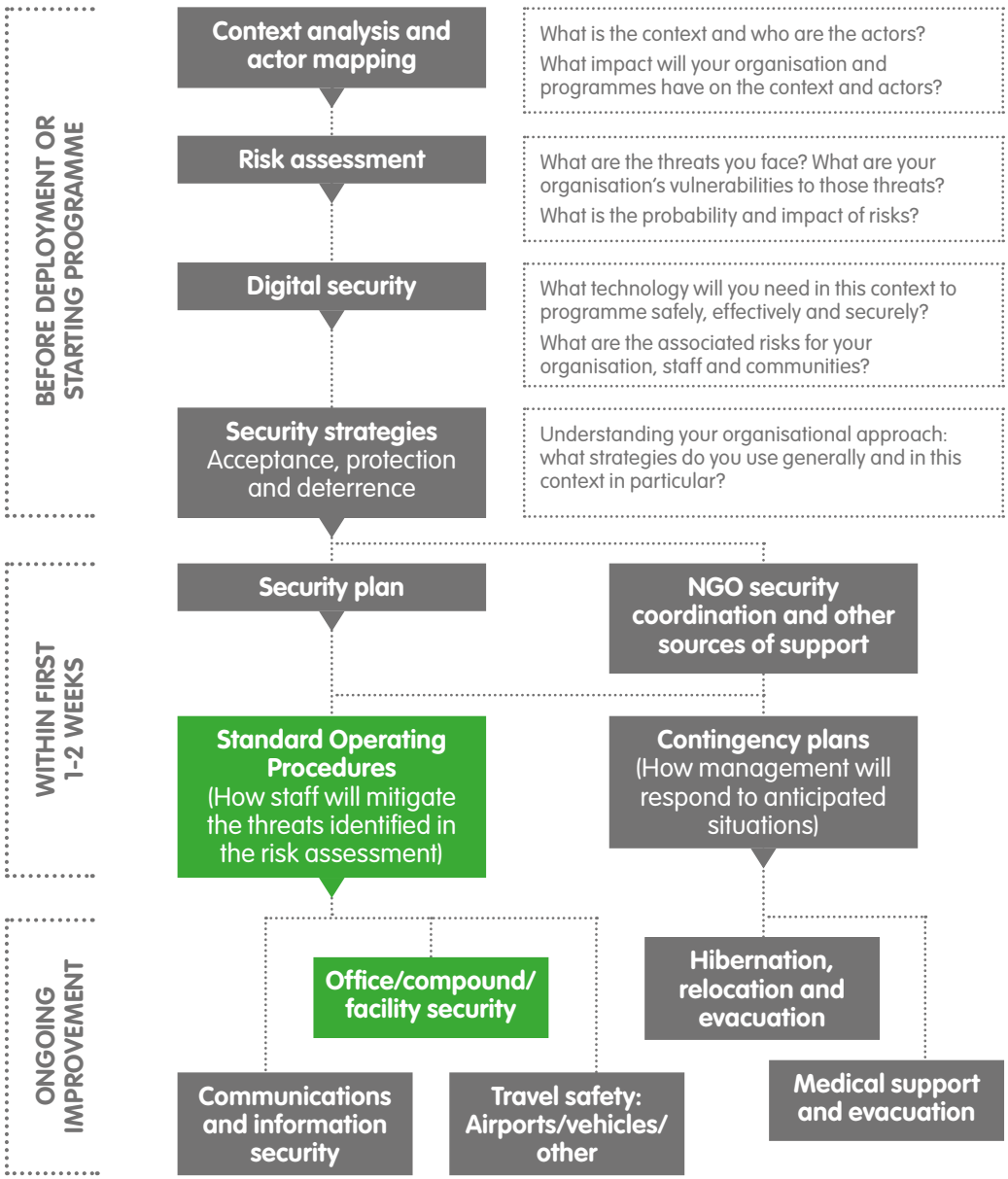
Who is in your crisis management team (CMT) and who they report to? How the CMT will be activated?

Include as well contingency plans for crises you suspect may occur such as kidnappings, natural disasters, evacuations, and armed conflict. Unlike SOPs, contingency plans are a management tool and are not for general distribution.

▶ *See Module 11 – Hibernation, relocation and evacuation*

▶ *See Module 12 – Medical support and evacuation*

8 Security of facilities



When considering a new office, residence or compound, first review your risk assessment to understand what the types of threats are, what the threat level is and what level of protection or deterrence you will likely need. This also applies if moving into an existing office with a partner organisation. Also consider if it will be possible to build an acceptance strategy in the location: this is often more difficult in large urban environments than in rural settings, though it is always advisable to create mutual understanding with your neighbours.

This is applicable to all organisational properties, offices, residences, warehouses, clinics, schools, etc.

In an emergency response it is often necessary and/or convenient to share space. If this is the case, it is important to agree who is responsible for what, i.e. perimeter security, guard services, local acceptance strategy, etc.

See EISF guide 'Office opening: a guide for NGOs'

Security of offices, compounds and other facilities

The outer ring: the neighbourhood

This is the area surrounding the office/compound/facility/residence. The risk assessment should identify who in the area could have an effect on the safety of staff. You need to understand your neighbourhood and the stakeholders within it to implement your acceptance strategy. It may be easier in rural areas than in urban environments, but developing understanding with your neighbours is essential in all contexts.

Consider:

- Road access, both access to the office and how you will safely travel to other sites. Is it a dead end? This can be positive for identification of hostile observation but will limit travel options/escape routes.
- Natural hazards like rivers (flooding), hills (mudslides/avalanches), swamps (malaria/dengue), or forests (fire, wildlife).
- Neighbours such as embassies, military/police posts, banks, government offices, other NGOs, or universities.
- Distance to airports, hotels, key locations in an emergency.
- Blocking structures/natural features that would interrupt satellite communications in an emergency.
- The landlord and his record and reputation.
- Reliable access to clean water.
- Access to telephone, the internet and mobile networks.

The middle ring: the property

This is the first area that is under the organisation's control. The risk assessment should guide you in how to secure it in terms of a perimeter wall, fence or hedge, or whether you leave it open, i.e. your protection strategy.

Always keep in mind that if you feel you need to build a 'bunker' to stay safe, you probably should not be based in that area.

When planning your perimeter you should consider how it may impact your neighbours and image, and the message it sends. If you decide to have a low profile and then wrap your compound in barbed wire, making it stand out from its neighbours, it will be counter-productive. You should also consider how your presence may affect your neighbours:

- Do you require a generator? If you do, can it be positioned away from other properties and/or is there room for soundproofing?
- Is there sufficient parking within the compound and/or in the area without without inconveniencing others?
- Is your presence creating a security risk for your neighbours?
- If you are employing guards, where will they be located?

It is possible to build protection measures that do not do not negatively change the appearance of the compound. For example barbed wire below the top of the wall, using flower beds or pots to disguise concrete barriers, etc.

Within your property there are other issues you will need to consider:

- Access control (planned): how do staff, visitors, suppliers or community members access your property? Consider vehicle/personnel gates, identity checks, safe parking areas, ID cards, waiting areas, and crowd control (if applicable).
- Access control (unplanned): how easy is it for people to get into the site? Are there shared boundaries with neighbours or open spaces? Are there overhanging trees and how close are the buildings to the boundary walls?
- Fire hazards including storage of fuel and combustibles, electrical power lines and designated smoking areas.
- How is trash collected and dealt with in a safe and environmentally sound way?
- Emergency exits: If your compound has a wall and main gate facing the street, how will you evacuate unobserved if there is a danger in front of the facility? Where will you go? Perhaps to a neighbouring compound/ UN facility/other NGO/residences?

The inner ring: the building(s)

Security for the organisation's buildings, whether they are offices, compounds/ warehouses or residences, is key as these hold your most valued items including people, equipment, assets, cash, records, and aid materials and supplies. The design of the building should also be appropriate for the natural hazards, e.g. earthquake resistant, insulated against heat and/or cold for heat and/or cold.

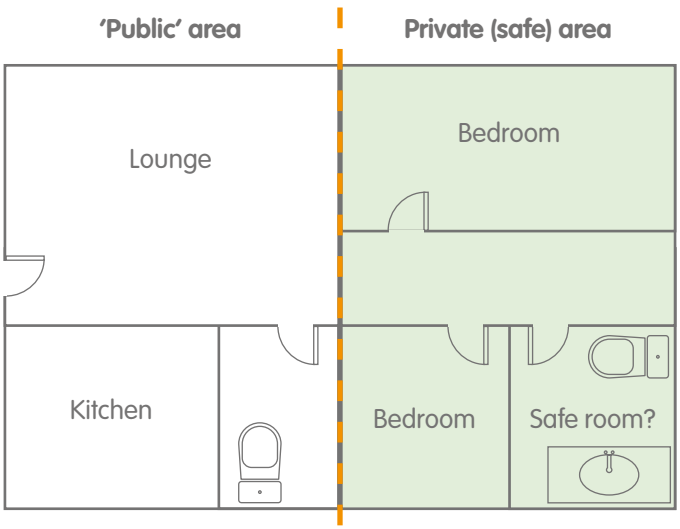
For staff to be effective in their work, it is important for them to feel safe in their office and accommodation. Consider:

- Security of doors/windows that prevent unauthorised access but do not trap staff in event of fire/evacuation.
- Security of roof areas (often a preferred entry point for robberies after hours).
- A reception area that controls access to other vulnerable areas.
- Access control procedures so that visitors admitted to the building cannot roam around unsupervised.
- Scheduled electrical inspections to reduce fire risk in addition to strict policies on not overloading electrical outlets.
- Safe storage of documents including fireproof safes secured to the wall or floor.
- Emergency evacuation routes and procedures clearly posted and rehearsed.

- If necessary, a safe room that will fit all staff expected to be in the building and equipped with emergency supplies (first aid kit, torch, blankets, food, communications device(s) that are charged/powered, fire extinguisher). Check that the emergency communication equipment works in the safe room. Satellite phones normally require line of sight, so external aerials may be needed.
- Uninterrupted Power Supply (UPS) units to protect computers and other electrical devices when power supply is not reliable or subject to spikes and power cuts.
- Alarms for fire or intrusion, and actions to take on hearing them, including rehearsals.

Security of staff residences

Staff residences can be approached in a similar fashion to other properties, but with some additional precautions to ensure safety. While the whole residence needs to have adequate security, valuables (TVs, computers, appliances etc.) are usually held in the 'public' areas of the house where guests or friends may be entertained, and these items are likely to be the principal lure for thieves. Private areas of the residence will include sleeping areas. These need to be secured to a higher standard than the 'public' areas.



Consider:

- A solid, lockable door between the public and private areas of the residence.
- Improved window and roof security in private areas, lockable from inside but not an obstacle in event of a fire for evacuation.
- A safe room with first aid kits, blankets, torch, fire extinguisher and a communications device that is charged and tested regularly.
- Window screens to keep out mosquitos (for prevention of diseases).
- Firm control of keys and any duplicates.
- Exterior lights, especially around entrances.

It is also important to consider local culture. In a conservative environment you may need to consider separation between male and female quarters, as well as separation between national staff such as guards and drivers, and international staff – so that international staff can relax without giving offence or the wrong impression by drinking and dancing, women wearing shorts, etc.

Watchmen and security guards

Many organisations look to locally engaged watchmen and/or security guards as a first step to developing their security systems around facilities. Organisations often use the term 'watchmen' rather than 'guard' to support the understanding that staff are not expected to risk their own safety to protect the compound and assets.

Guards are often the first point of contact between the host community and an NGO. How they behave, their manners as well as professionalism will often reflect back on their employer. Therefore, for all guards or watchmen ensure the following:

- They are aware of your organisation's mandate and Code of Conduct.
- They are given clear instructions on their duties and how they will be supervised.
- Guards have a list of 'actions on' to deal with visitors, suspicious activity, robbery, fire, injuries or other incident likely to occur, as identified in your risk assessment.
- Ensure staff members treat guards with respect as well as understanding of the guards' duties, and ensure compliance.
- Guards should be given an emergency contact list and means to communicate if an incident should occur.

▶ *See EISF briefing paper 'Engaging private security providers: a guideline for non-governmental organisations'.*

Virtually all NGO guards are unarmed. However, in high-risk environments it may be common for organisations to have an armed response in case of emergency, either activated by panic buttons or existing guards. If this is the case the organisation should get information about who provides the armed service (private company, police, military), what its purpose is (protecting the organisation's staff and assets or apprehending the attackers), their level of training, and the organisation's liability if someone (staff, guard, bystander) is shot during an armed response.

There are three main categories of security guards: commercial guards, contracted guards and community volunteers. Each has advantages and disadvantages.

Commercial guard services

They are provided by a contracted guard services company. The guard company may rotate staff making it difficult to create a level of trust. It is important, particularly in residence buildings, that staff members know the guard who should be opening the gate. Otherwise the guard can create feelings of insecurity rather than alleviating them.

Advantages	Disadvantages
The provider can supply additional services such as a rapid response team (be clear on what this involves), alarms, radio networks, vehicle patrols, and night supervisors.	The organisation has little or no control over the guard's instructions and duty standards.
Recruiting, training, payroll, HR, admin and scheduling are done by a commercial provider.	Security companies are mostly concerned with 'the bottom line'.
	Guards are poorly paid and unmotivated.

Contracted guards

They are employed directly by the organisation.

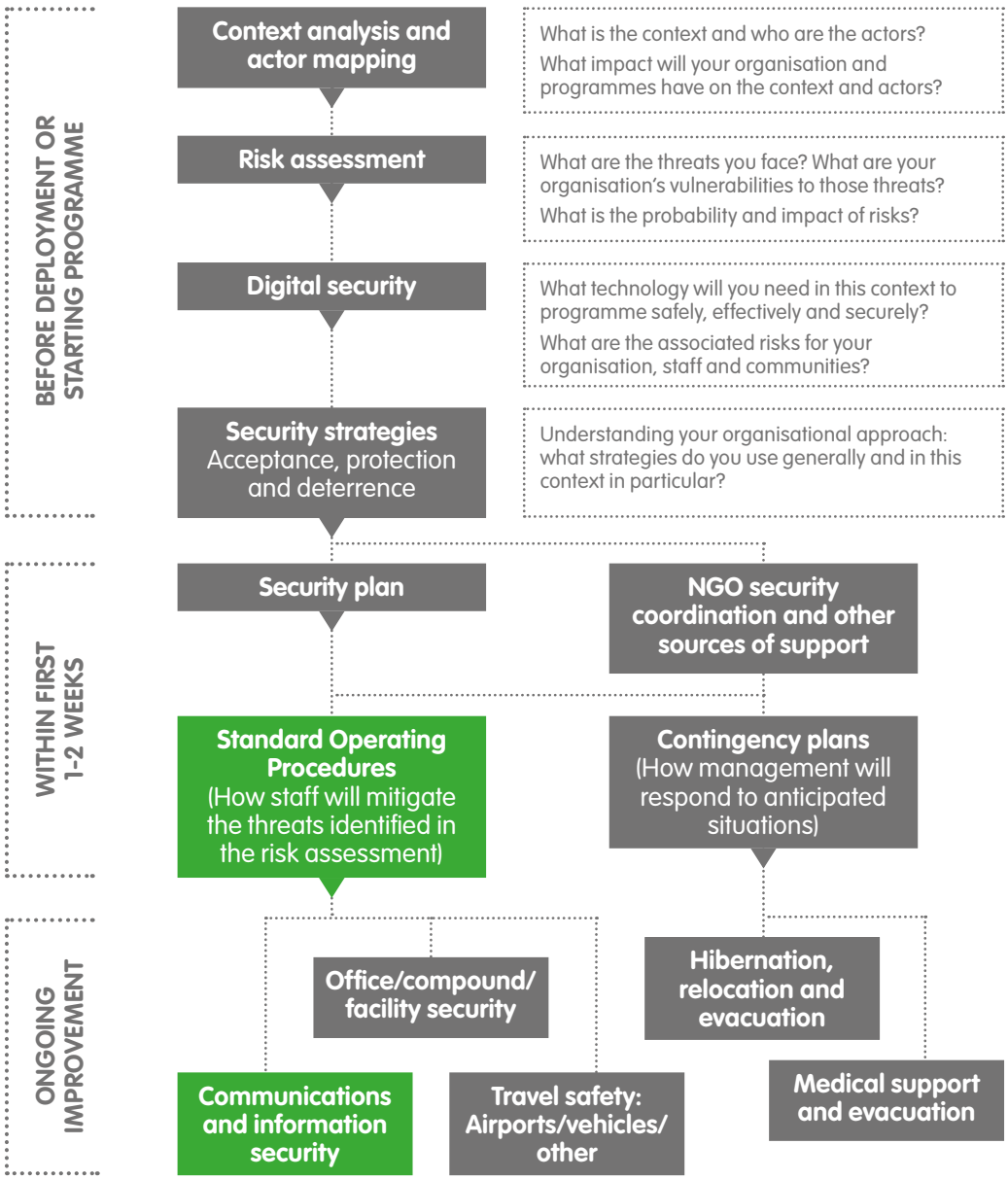
Advantages	Disadvantages
Guards can be better paid since the money of the aid agency does not go to the commercial profit system.	The organisation must take responsibility for training, uniforms, equipment, administration and supervision.
As members of staff, they have increased loyalty and knowledge of the organisation's standards, policies and code of conduct.	No additional support available.

Community volunteers

Normally, they are guards provided by the host community in programme areas. They are often the only option in remote areas. There is normally a cost for salaries, training, minimal equipment.

Advantages	Disadvantages
Utilises 'acceptance strategy' approach by incorporating the community into security.	No set standards for duties.
	Lack of accountability.
	Open to abuse.

9 Communications and information security



In setting up any new deployment, project or mission, time must be taken to consider what types of communications will be available (landline, mobile networks, satphones, internet, surface mail, courier, etc.) and how reliable they are likely to be. In the modern world, communications are as much a key 'survival' need as food, water and shelter.

Budgeting early for reliable communications systems – including back up and alternate systems for replacing damaged, lost or stolen equipment – is a key component of both staff safety and programme success. Also, some forms of communications such as radios or satellite systems may require licences to operate. The United Nations may be able to give support in obtaining licences. The organisation should budget for airtime and/or licencing where necessary.

Be aware of new technologies that can cost effectively improve your communications such as satellite 'back-packs' for smart phones or satellite messaging systems rather than traditional voice phones. Buy the best you can afford.

However, organisations need to consider the image their communications equipment conveys. If having a low profile is part of the security strategy, adding HF radios and aerials to vehicles will make them stand out as much as a logo.

In regions of conflict, civil unrest or after natural disasters, never assume the internet and mobile networks will be reliable. During security emergencies or natural disasters, governments often take control of (or shut down) networks – at the time you will need them most. It is important to never rely only on a single system whether it is landline, mobile networks, satellite phones, the internet or others.

Be creative. In emergencies, NGOs have used relays of taxi drivers to maintain communications with staff when phones or the internet were down, or used camels to carry messages and maintain contact with remote communities.

Communications security and procedures

Establishing and maintaining an extensive communications network is key to safety, security and success of operations. If you have radio networks or satellite phones, train staff in their use as part of their induction and inform them about where the installed communications equipment can be used (e.g. do you need to be outside? Are there black spots?). Ensure attention is devoted to staff being able to communicate with family and friends during deployments, and especially in emergencies.

A growing number of organisations and coordination bodies are using WhatsApp and other similar social apps for sharing information directly between staff. This can bring great advantages for sharing information in real time, however information in these networks is unverified. There should be clear guidelines on what information can or cannot be shared, and the procedures to follow for acting upon the information received.

In general, all communication procedures and guidelines should be discussed with staff. Written procedures, as well as essential emergency contact information, including phone numbers, frequencies, and call signs should be posted in the office, each vehicle, and on a card for each staff member to carry.

It is important to test the systems regularly and have back up power supplies for radio, mobile/satellite phone charging.

Good practice:

- Staff never transmit sensitive information, such as the transfer of cash or travel plans, in plain language over the radio or phone networks.
- Communications equipment, including radios, cellular phones, and satellite phones, have the host nation government's approval and licensing prior to use.
- Where radios are used, multiple VHF and HF frequencies have been obtained for each office when possible.
- Use of other organisational radio networks – such as the United Nation's – has been coordinated.
- SMS, satellite phone calls or radio checks with remote offices and travellers in the area are routinely performed, as appropriate. A policy is in place in case a staff member or team fails to check in and cannot be contacted. All staff are familiar with this policy, and it is consistently implemented.
- Duress code words or phrases have been established for common emergency conditions such as kidnapping or intrusion. Their use has been discussed with staff.
- Radios and emergency phones are monitored 24 hours a day, as appropriate.

Information security

Regardless of how we view ourselves, international aid organisations are often no longer regarded as neutral, independent entities. They intervene, hold accountable, advocate and often subsume activities normally associated with governments (such as health care, water, sanitation and emergency relief), and in many occasions undertake these activities while funded by 'Western' governments with their own political agendas. This makes everything humanitarian NGOs do seem suspicious in many people's eyes.

▶ *See EISF briefing paper 'The future of humanitarian security in fragile contexts: an analysis of transformational factors affecting humanitarian action in the coming decade'*

Governments usually have the means to monitor organisations' phone calls, internet activity, Facebook, Twitter and RSS feeds as well as hack your computer hard drives. Criminal organisations will also perceive NGOs as wealthy, given the vehicles, laptops, satellite phones they often use, as well as publicly announced donor funding levels. All of this makes aid agencies vulnerable to information security risks. Be aware that anything you write in an email can be read by criminals or government agents.

▶ *See EISF briefing paper 'Communications technology and humanitarian delivery: challenges and opportunities for security risk management'*

Consider what to put into any shared drive. Emergency response staff often bring their own computers and will copy everything into a shared drive when they leave, for continuity. This may include inappropriate photos, personal information and context analysis that may be deemed insulting by other actors or staff. It is important to keep in mind as well what information – both business and personal – is kept on mobile devices such as smart phones, as this might easily be lost or stolen.

Assess the impact the information might have if it falls into the wrong hands – harassment of staff, dissemination of inappropriate photos, access to emails or office VPN/server, and so on.

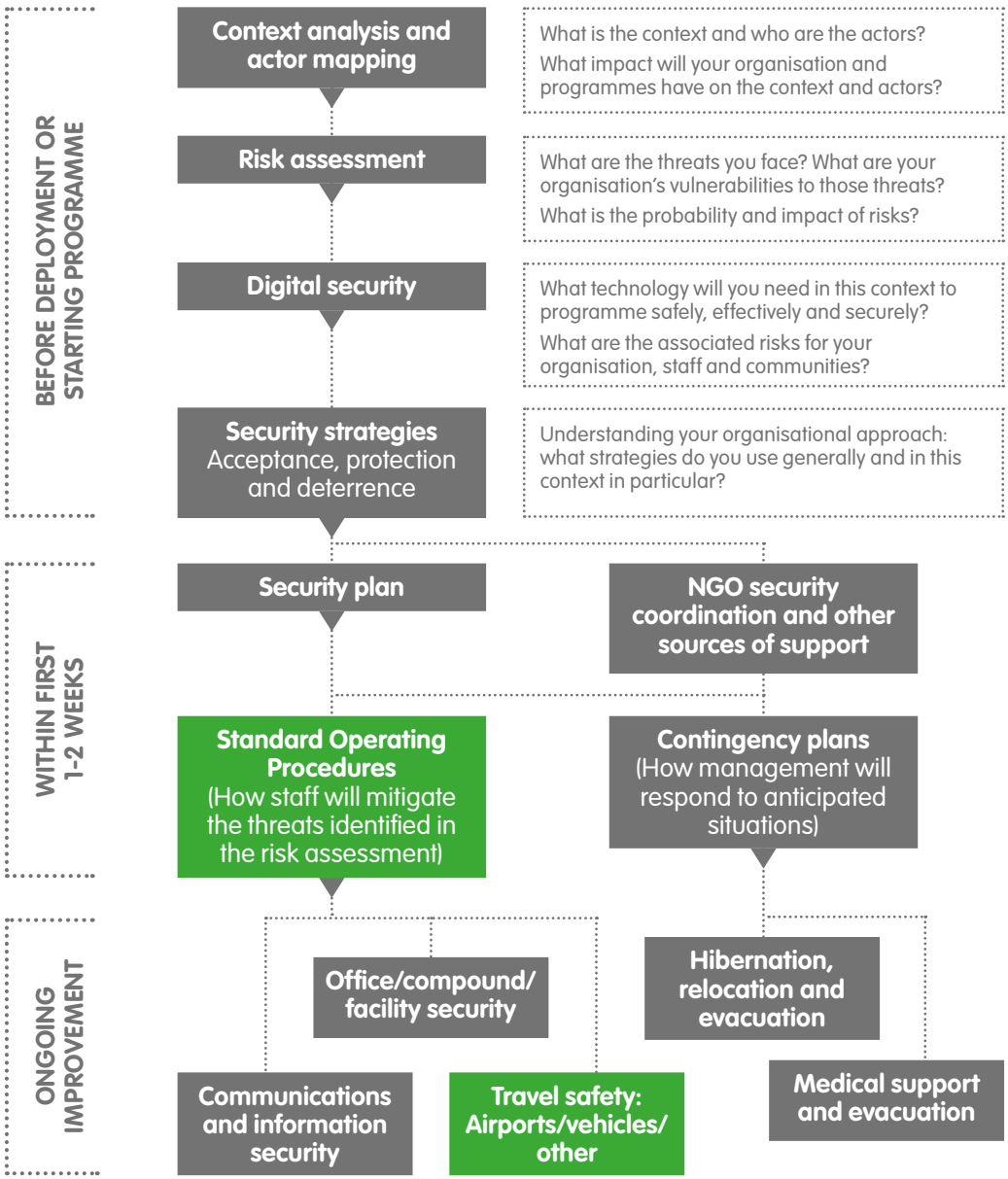
Good practice:

- Back up all files regularly and keep back up copies of all key documents and records (government agreements, legal documents, bank records, HR records) off site in case of fire, flooding, theft or other event that destroys the originals.
- Paper documents also allow information leaks if they are left in bins or on desks for cleaners and other staff or visitors to see/copy/remove. Use shredders for any files not being kept in safe storage.
- Maintain good security firewall systems in any server and minimise staff access to networks with non-organisation computers, tablets or phones to prevent spread of viruses.
- Remember that Skype is no more secure against hacking than any other communication method.
- Never appear to be gathering 'intelligence' or passing any military or security information to foreign governments (including donors or your headquarters). Similarly, encrypting information may send the wrong message. Particularly if your NGO claims to be open and accountable, you may be questioned about the need to encrypt documentation.
- Avoid desktop computers when possible. Although laptops are easier to steal they are more mobile if the office or project needs to be relocated.
- Consider verification processes for information received via WhatsApp and other social apps that make it easier to share information directly between staff. There should be also clear guidance on what should and should not be shared.
- Ensure you have a social media policy that makes it clear to staff what they can and cannot post on social media sites.

▶ *See EISF guide 'Managing the message: communication and media management in a security crisis'*

For technical tools and guidelines, 'Front Line Defenders' and 'Tactical Technology Collective' have developed *Security in-a-Box*, a guide to digital security for activists and human rights defenders. The guide covers the basic principles, including advice on how to use social networking platforms and mobile phones more safely, and also offers step-by-step instructions on how to install and use the most essential digital security software and services.

10 Travel safety: airports, vehicles and other means of transport



According to the *Aid Worker Security Annual Report 2014*, of 795 aid workers killed between 2006 and 2013, 263 (33%) were killed in road ambushes. Travel is the time when NGO staff are most vulnerable to robbery, assault, kidnap, corruption, injury or death. This includes air travel between countries, travel by road from the airport to the office or accommodation, from office to residence, to and from field projects and meetings, and anywhere else that staff find themselves moving between secure locations.

Good practice:

- Make sure that you can be contacted as much as possible when travelling.
- Leave a copy of your travel itinerary, key documents and local contact details in case direct communication cannot be established.
- Confirm all visas, invitation letters, local currency, addresses and phone numbers prior to departure.
- Make copies of all important documents with you, such as passport, visa, insurance card and credit card, and leave them with the point of contact in your department. In certain cases, it may be useful to carry a copy of your passport (including any visa pages) and to keep the original in a safe.
- Email yourself a copy of important documents so you can easily access them online from any computer.
- Obtain an international driving licence, if required.
- Take your vaccination records with you.
- Consider whether you need medical/evacuation/other insurance.
- Investigate whether there are any health preparations you should take (such as medications, first aid kit, water purifier).

It can be useful to run scenario-planning exercises before any trip, particularly when travelling to a new area or a fluid context with a changing environment. All staff involved can discuss possible scenarios and responses to them, and be better prepared if something happens.

When travelling on business, you should ideally be given a personal organisation identity card. With this ID card, you are quickly able to show that you are travelling on behalf of the organisation. The card is not a formal means of identification, but can be very useful in making known the purpose of your visit and, if necessary, providing you with a specific status for your visit. Always carry the ID card with you. If necessary, you can also take a letter of guarantee with you. This letter should outline the purpose of your visit and who you will be visiting.

Travelling by air

When crossing long distances, air travel is often unavoidable. For air travel, especially regional and national travel, it is important to consider the safety record of the airline selected and whether they are IATA, EU and FAA certified, otherwise your insurance coverage may not be valid. Some websites that can be used to consult airline safety records are FlightSafe, SkyTrax and AirlineRating.

Good practice:

- Choose aircraft with more than 30 seats where possible. Normally, these must adhere to stricter safety regulations and more stringent manufacturing standards.
- Choose non-stop flights as most accidents occur during take off and landing.
- Sit near an exit and memorise the location.
- Choose aisle seats when possible so that you can get up and move faster in an emergency. This is also better for circulation, so that you can get up and stretch when possible.
- Do not drink alcohol (or minimise intake) as cabin pressure increases the effect of alcohol on the body.
- Know what is and is not allowed in carry-on baggage and be prepared to have it searched.
- Never leave carry-on or checked baggage unattended.
- Pack your carry-on bag with all the key items you will need to survive if your checked baggage is lost, damaged or delayed.

On arrival to the airport, travellers should have a contact list for key people and know what to do if a driver is not immediately apparent – where does the traveller wait? Should you then get a taxi or not? And if so, what type of taxi? Travellers should have a way to contact headquarters and local staff at their destination in case of a problem, such as a flight delay or missed connection. Details of the meeting point and transport from the airport need to be agreed before travel, and be part of the security brief any staff should have prior to departure.

Depending on the context, travellers should be provided with the name and photo of the driver or a way to identify the correct driver. Drivers should display a card with the organisation's logo rather than the name of the traveller. Displaying the name makes it easier for others to approach the traveller, and the name can also be easily duplicated on a fake card or sign.

Travellers should receive an updated security briefing as soon as possible after arrival and be give a card with key phone numbers and locations on it.

Travelling by road

If purchasing or hiring your own vehicles, ensure they are the right type for the work you will be doing. Consider your risk assessment regarding branding, visibility, theft rates per vehicle type, road and terrain conditions, spare parts availability and other logistical issues.

When hiring vehicles, you should consider whether to hire the vehicle with a driver or use instead the organisation's own staff drivers. In the latter case, all staff members operating a vehicle should be able to perform basic maintenance, such as changing a tyre and checking engine, brake, battery and radiator fluids. If planning to travel in local partner vehicles, ensure you review their driver training and supervision policies, vehicle maintenance records and travel security procedures. Drivers should observe local driving laws and regulations, and drive at speeds suitable for the conditions. Passengers are also responsible for ensuring this is the case.

All staff – both national and international – should also be briefed about the policy concerning unauthorised passengers, especially soldiers or armed militia. Similarly, a clear policy concerning the use of vehicles for personal use during and after the workday, weekends, and holidays should be in place and all staff members briefed on it. National and international staff should all have proper travel documentation, including driver licences.

When travelling, all occupants of the vehicle (including the driver) should know the same basic information about the organisation in case they are stopped and questioned separately. Additionally, make sure a spokesperson has been identified prior to departure.

When possible, staff should travel with at least one other person. Travellers need to notify others of travel time and destination according to the established procedures. A communications plan details check in times and missed call actions, and vehicle accident procedures are also in place and all staff briefed. If staff do not arrive as scheduled, the agreed communications policy should be consistently implemented.

Module 9 – Communications and information security

To ensure timely reporting during travel, it is key that all mobile phones are fully charged and work in the area where the mission is going to be conducted. If that is not the case, alternate communications equipment and protocols should be considered. When evaluating different systems and protocols, it should be kept in mind that these may vary depending on the route chosen. If there are route options, select primary and alternate travel routes to avoid danger areas and adapt to changing security conditions. It is helpful to keep an updated country or regional roadmap in the office with dangerous areas marked as well as areas where mobile phone signal is unavailable.

Good practice:

- Vehicles are equipped with basic tools, spare tyre, tyre changing equipment, first aid kit, blankets, emergency drinking water (2 litres per person per day), emergency triangles, torch, fire extinguisher and anything else needed given the local geographical/climatic conditions.
- Seat belts/shoulder harnesses should be fitted and working, and always worn in both front and rear seats.
- Vehicles are checked daily. Someone has been designated as responsible for maintenance and correction of discrepancies.
- Essential vehicle registration and documentation is in each vehicle.
- Helmets are worn by anyone on a motorcycle at all times.
- Vehicle fuel tanks are maintained above half full if possible.
- Spare vehicle keys are kept under strict control in each office.
- Vehicle doors are kept locked while driving and the minimum number of windows opened.
- Vehicles do not have darkened or tinted windows that may obscure visibility.
- The use of travel forms, trip tickets or a vehicle tracking system is in place to help track vehicle movement.
- The appropriate emergency contact details for all relevant individuals, organisations, hospitals and police stations in the area are posted in each vehicle.

It is also good practice to maintain logbooks for each vehicle and keep a copy on the vehicle of the checklist and maintenance schedule, trip tickets, communication procedures, documentation, maps, etc. However, consider how this information may be received if it is discovered when a vehicle is searched at checkpoints.

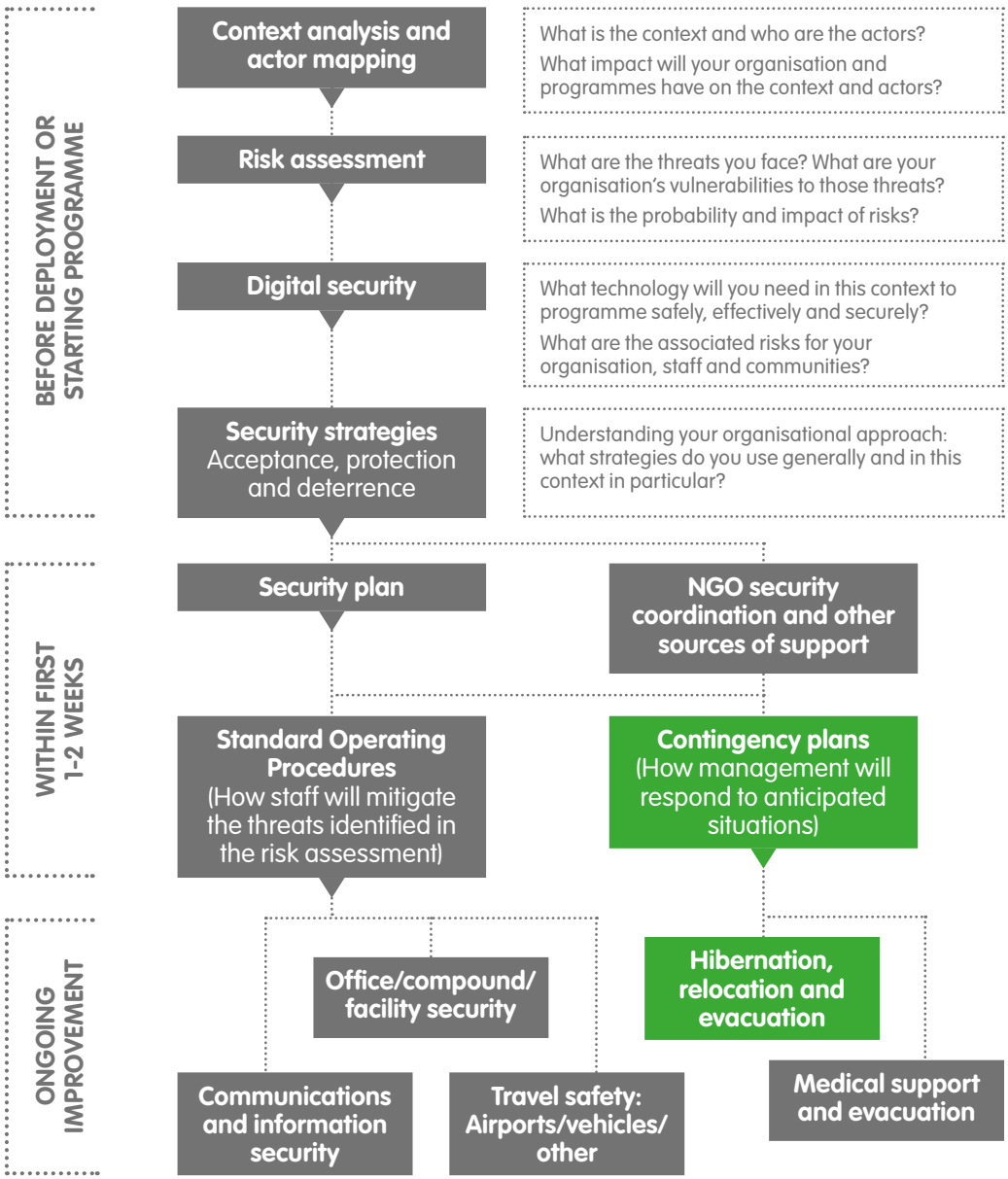
Other transport modes

In some contexts it will be necessary, or cost-convenient, to use alternate forms of travel. These can include boats, trains, helicopters, public transport and taxis. For each mode of travel, do a short risk assessment, including researching the risks and developing mitigation strategies for each.

For boat travel especially, organisations may need to take extra precautions. It is important to make sure that either the boat operator or the organisation supplies items such as life preservers and Emergency Position Indicating Radio Beacon (EPIRB) units. The organisation may also need to provide swimming or lifesaving training.

For public transport consider the needs of national staff as well as international staff for to and from office, during and after working hours, and for R&R and/or leave.

11 Hibernation, relocation and evacuation

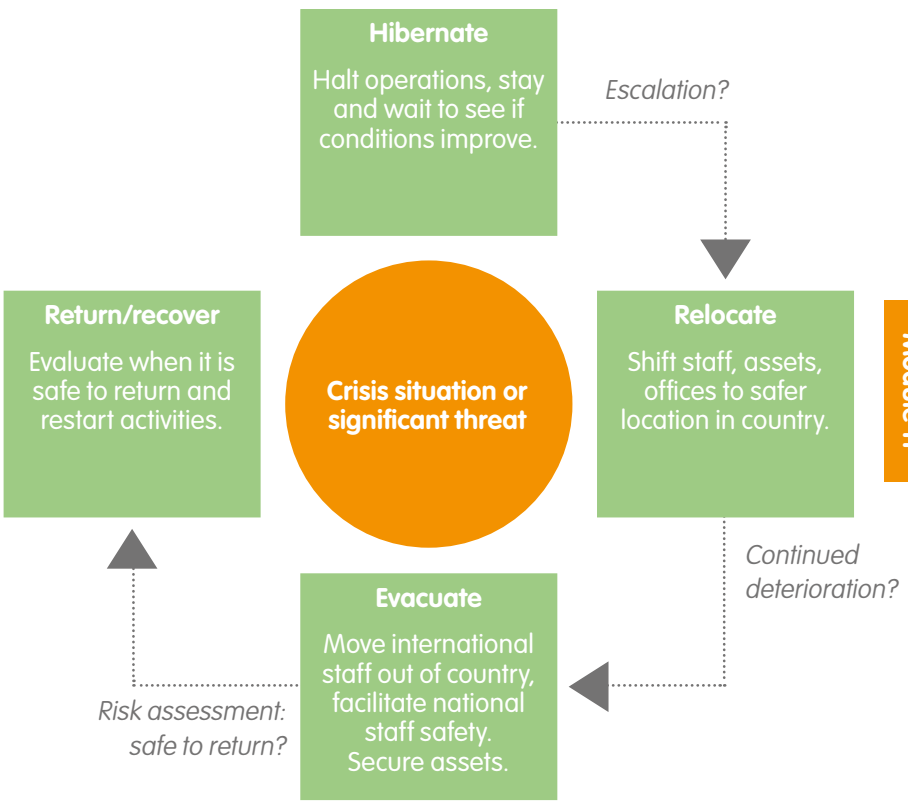


Aid agencies often work in regions where natural disasters occur or conflict threatens the human environment. As such, it is important to put some thought into how your organisation will react to a situation where it becomes unsafe for a short or extended period. There are typically three levels of reaction to a significant change in the threat context:

Hibernation: Staff stay at home and there is a temporary halt to programming during a crisis period. In some circumstances, staff may be required to shelter in the office or compound.

Relocation: Shifting offices and/or activities from an unsafe area to a safer location, usually on a temporary basis and within the same country.

Evacuation: Suspending operations in a country, evacuating internationals to another state and national staff from deployed areas to their home areas. Some limited programming may continue using remote management, depending on the situation.



It is important to identify 'triggers' that can be agreed upon between in-country staff and headquarters to determine when the various contingency plans should be activated. For example, for flooding, when rainfall levels reach a historic level that normally results in flooding, hibernation or relocation contingency plans can be activated. If armed conflict in another part of the country expands to an agreed upon line or area, relocation contingencies can be activated.

▶ *See Glossary*

By agreeing these triggers in advance, all in-country staff, host government, headquarters and donors will understand your decision. However, it may not be appropriate to share these triggers or resultant actions with particular actors. For example, when considering where you might relocate activities if armed conflict comes too close to your current location, it might not be appropriate to share this information with actors in the conflict in case it affects their decisions or increases your vulnerability as a target.

It is important that, as far as possible, triggers are developed when the situation is calm. If decisions are made during the heat of the crisis, peoples' perception of risk will affect the decision-making process.

While no two crises are alike, there will normally be some warning that the situation is deteriorating or a natural disaster is imminent. While some natural disasters occur with no warning (as is the case with many earthquakes), for others, like tropical storms, flooding or deteriorating conflict, there is usually some warning or indicators. Each contingency plan should have three phases:

- Warning phase: alerts all stakeholders that it is time to prepare.
- Activation phase: sets the contingency plan into motion.
- Recovery phase: details how the organisation will return to operations safely.

Re-location and evacuation of staff may be phased, with different triggers applicable for different staff. For example, in an area subject to flooding the triggers might be: heavy rain for six days with possible flooding, no essential staff relocated; heavy rain for eight days and rivers reaching an agreed level, all staff relocated.

Defining essential staff will vary between organisation and context, and may also vary for different risks. Role, programme, experience and personal risk appetite will all play a part in the identification of who essential staff is. Ethnicity and nationality should also be considered for conflict-related risks.

Most organisations have a 'free to go' policy where individuals have the right to relocate or evacuate if their personal sense of risk is exceeded. Individuals should be made aware of organisation's policies in contexts where relocation and/or evacuation may be required.

Hibernation

Good practice:

- Ensure offices have stockpiled emergency food, water and first aid supplies for anticipated number of people and agreed period of time.
- Stockpiled supplies should be appropriate: non-perishable, portable and nothing frozen as it can go off if the generator breaks down.
- Stockpiled supplies should be accessible (e.g. in places at risk of earthquake, do not store supplies in an area that is safe from theft but prevents staff from retrieving the supplies in case an emergency – in this case, an earthquake – happens).
- Have appropriate communication equipment at hibernation location (e.g. if you are moving into an enclosed safe room, a satellite phone will not work).
- Have a back-up generator and fuel, if applicable.
- Pay staff 2-3 weeks salary in cash to allow them to survive.
- Contact suppliers, banks and advise them of your plans.
- Have staff work from home but check in daily and advise on their situation and observations.
- Minimise activity in office, back up key files offsite, and disable vehicles if there is a threat of theft during chaotic periods.
- Liaise with other NGOs in similar situations.
- Maintain contact with communities to gather information and let them know they are not forgotten.

Relocation

Good practice:

- Identify in advance locations that you can temporarily relocate to if the operations centre or a specific region becomes unsafe to work in. These can include:
  - Existing field offices
  - Other NGO compounds
  - Guest houses
  - Other secure locations
- Ensure that the temporary location has suitable phone and internet access.

- Maintain good communications with communities so that they do not feel abandoned and thus damage your acceptance strategy.

See Module 5 – Security strategies: acceptance, protection and deterrence

- If staff members have been relocated, ensure that any evacuation contingency plans are updated accordingly, in case the situation deteriorates further. If staff are registered with the United Nations, the embassy or insurance company at a particular location, make sure that the information is updated.
- Ensure national staff and their families are also taken into consideration so staff are not asked to leave their families in dangerous areas while they go to work in safety.

See EISF guide 'Office Closure'

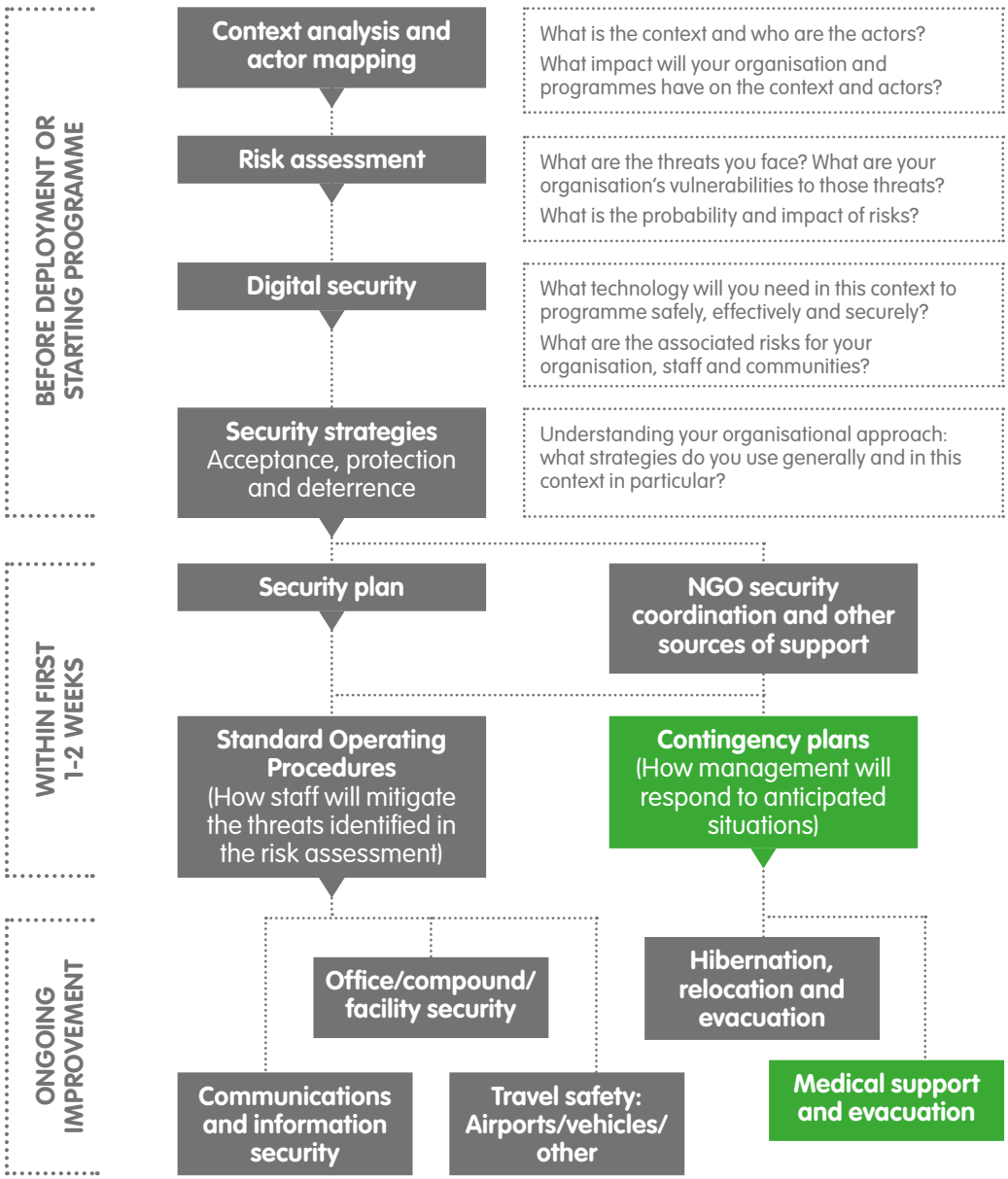
Evacuation

Good practice:

- Do not focus entirely on international staff. National staff hired in one area and employed in another (re-located staff) are often at far more risk than internationals. Ensure nationals are internally evacuated to their home areas prior to pulling out.
- Do not promise to evacuate national staff. It is not the role of NGOs to create refugees nor is it legal to employ staff in a third country.
- Pay staff one month's salary in cash prior to evacuation.
- Establish communication channels with remaining national staff and communities to assist in determining when it is safe to return.
- Plan how assets such as vehicles and computer equipment will be secured in-country or legalities of moving them to a neighbouring state.
- Do not rely on the United Nations to evacuate your international staff. Make your own arrangements.
- Do not rely on promises from embassies to evacuate all your staff, especially if the international staff member is not a citizen of that country.
- If you have insurance have clear details of what it covers. For example, it may specify a particular standard of runway which is only available in the capital city.

Once staff have been evacuated it can be very difficult to return to the same location. When developing the contingency plan for evacuation, consider indicators for return as well as how to maintain relationships previously developed with different stakeholders. Evacuations should always be considered as last resort measure.

12 Medical support and evacuation



Medical risk and needs assessment

When organisations deploy to a new country, or region within a country, it is important to assess what health risks – both physical and mental, including stress – staff may face. This medical threat or hazard assessment will inform your preparations. Beyond universal medical conditions, medical threats could be grouped in the following types:

- Ballistic trauma
- Sexual violence
- Road traffic accidents
- Disease (endemic and epidemic)
- Hygiene
- Psycho-social
- Environmental (wildlife, heat, altitude)
- Chemical, biological, radiological, nuclear

It is equally important to assess the medical assistance available and its capacity to respond – including the infrastructure – as well as considering insurance and gender-specific issues that may arise.

Medical assistance and capacity to respond

- What level of services are available? (e.g. emergency, surgery or palliative care?)
- Are drugs available? Do patients need their own needles, syringes or antibiotics?
- Are medical facilities capable of dealing with common serious ailments such as heart attack, other organ failure, or similar medical emergencies?
- Are there medical NGOs in the area? What medical services are they able and/or willing to provide to your staff?
- Are there ambulances? Are they reliable? Can they reach remote locations?
- If no ambulance service is available in your area of operations, or it is unreliable, how will injured staff be evacuated?
- If you have to consider self-evacuations it is strongly advised to train staff on how to do this safely.

Infrastructure

If air evacuation in-country is an option, establish a relationship early and understand the requirements of the service:

- How do you give locations for medevac requests (using GPS latitude and longitude, MPRS, other?)
- Are there pre-registered evacuation locations in the area already?
- What type of aircraft does the service use and does it need paved/dirt airstrip or clear ground (an area of what size?) for a helicopter?
- How do you stabilise/secure casualties for evacuation?
- How do you communicate with aircraft?
- How do you record/secure identity documents and treatment information for casualty?
- Where will a casualty normally be taken?

Insurance

Organisations will normally have medical insurance. This may be a standard policy for national staff and possibly include medical evacuations for international staff. It is important that all staff are fully briefed on these policies prior to deployment and know their policy number and contact details of the insurer. Some organisations require consultants to provide their own health insurance.

Ensure administrative staff in-country are aware of insurance provider arrangements and cover for all staff – including consultants, secondments and volunteers – particularly if international staff and/or visitors from headquarters have different medical insurance providers.

Maintain records of the insurance policies in case of emergency and establish a system in place for sharing the specific information with in-country staff, e.g RED form. If the insurance provider has pre-approved specific hospitals and/or doctors, it is advisable to visit these locations and establish a relationship and communications channels locally. It is important to understand the procedures for admittance into the approved hospital – just because the hospital is approved by the insurance company, it does not mean staff will automatically be admitted.

Following a bomb blast (…) a number of foreigners from two different agencies were injured. All staff members were taken to the same initial triage location and had the same medical insurance provider. One agency had pre-visited the hospital administration and had developed a relationship; its staff members were admitted into the hospital within approximately one hour. The other agency followed the procedures as identified by the medical insurer, and it took over three hours to get its staff admitted into the same hospital.

Some other points to consider are:

- Does the medical insurance approve hospitals and/or doctors for the area?
- Are there any restrictions in the coverage (e.g. communicable diseases)?
- Are all staff covered under the same policy (national, international, secondments, consultants and volunteers)?
- Are there restrictions on types of medical evacuation the insurance can undertake? Where are these available in relation to the risks faced? For example if they require a particular type of runway for air evacuations.
- Does the insurance provider have specific evacuation points within the country? Where are they and how will the staff get to these points?
- Are stress injuries covered?
- Is counselling available for those who have suffered any form of mental/psychological trauma?

Gender-specific considerations

- Are there cultural restrictions on who can provide first aid, based on gender, either amongst your staff or within the local population?
- Are there gynaecological and obstetric services? Are contraceptives available?
- Is pregnancy considered a high-risk condition in the host country?
- Are post-exposure prophylactics available?

Pre-deployment preparations

Once a medical risk assessment has been conducted and taking into account the above mentioned considerations, typical pre-deployment preparations and checks might include:

- Medical briefs, screenings (including mental health), checks, and vaccinations.
- Personal medical information (e.g. baseline vital signs, blood type, conditions, medications, GP contact).
- Personal medical supplies and first aid kits (date, sufficiency, and whether supplies can be imported into the host country).
- Equipment or supplies available and procured in-country.
- Required training (including refresher) for first aid or more advanced medical skills.

Medical contingency plans are easy on paper, but can often fall apart, only adding to the stress of an incident and worsening its outcome. The assumptions we make about logistics can be unrealistic, the plans can be inadequate, information becomes outdated. Invest your energy as soon as you can in medical contingency planning, before you leave and when you arrive, and test and update plans regularly, so that medical incidents do not become crises.

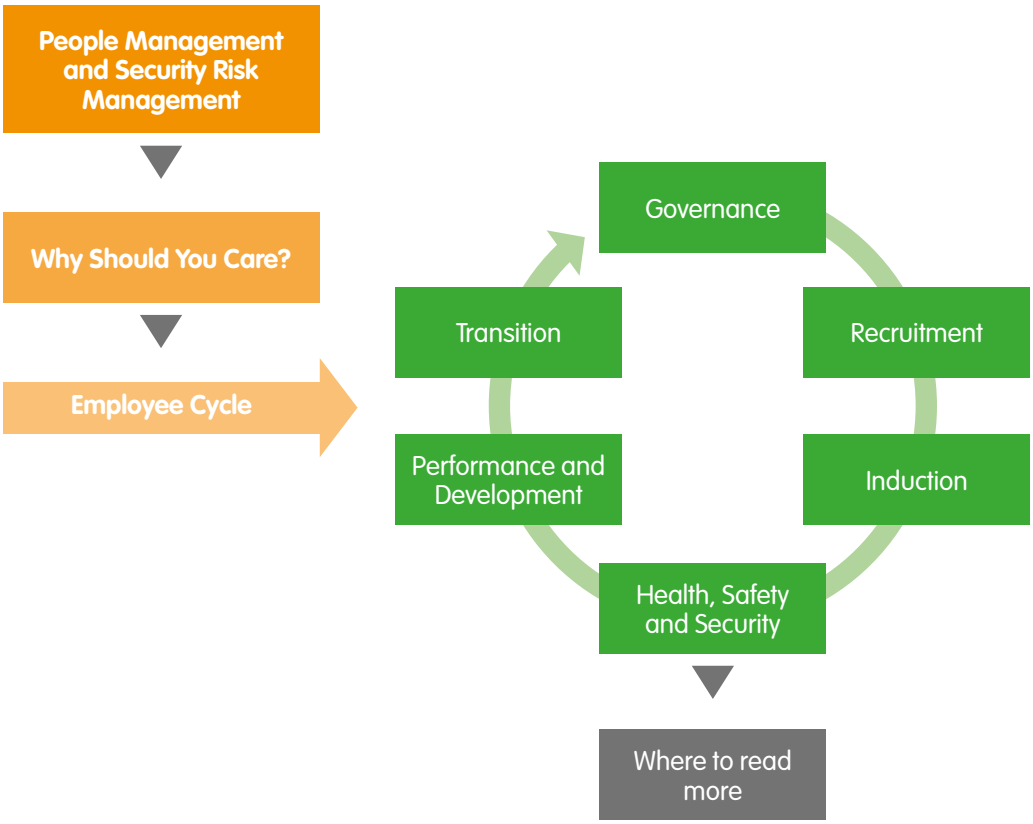
Team leaders should also specifically discuss with points of contact within the NGO the support, processes, and requirements the organisation has or offers. This might include:

- Crisis management plan and contingency plans for medical emergencies.
- Insurance coverage details (who is covered, what is covered, what the response is and its limitations, where the gaps are, what information is required and when, contact details).
- Previous organisational experiences of handling medical incidents.
- 'Clinical governance' (who is authorised to treat whom, to what level, including medications).

When deploying as a team, designate one member to be responsible for undertaking a more detailed medical risk assessment. For individuals deploying, identify the local contact point for medical support and get a full briefing. This should include:

- Who is trained, equipped, and available to provide first aid for all staff at all times?
- Who can provide in-field care to stabilise critical casualties and where are they located/how are they contacted?
- Who can appropriately transport casualties for emergency care, where and how?
- Who is overall responsible for controlling and coordinating at the country level (organisation, insurance provider, other)?
- Who will communicate what, to whom, when, and how?
- What information is required by insurance medical providers? By whom and for what purpose? For example, is a doctor's report required to initiate a medical evacuation?
- Does the United Nations or others, for example the ICRC, have the logistics capacity to carry out medical evacuations within the country? Is this service available to NGOs, and if so, how is it accessed?

13 People management



People management and security risk management

Good people management could be described as getting the best results from an employee in a healthy and safe way. People are our most valuable resource and if we believe happy, secure and motivated employees are more likely to be engaged, committed and productive, it makes good business sense to support employees well and to provide them with a healthy and safe working environment.

People management is a broad and complex subject that carries legal and ethical responsibilities for an organisation to ensure the physical and psychological health of an employee before, during and after the period of employment. Organisations have many legal and ethical 'duty of care' obligations and are expected to go above and beyond the legal minimum when working in high-risk environments.

Those in leadership positions – trustees, directors and managers – must invest time and resources in people management practices, and ensure technical specialists within human resources and security provide the necessary advice at the right time and in the right way.

People and security risk management – why should you care?

People management has a direct impact on security risk management, for example:

1. **Recruitment** – employing the wrong people can create security risks. A lack of skills and competencies can lead to poor performance and decision-making; poor behaviours can lead to personal and programme risks; and failure to consider the implications of the ethnic mix in some regions can create issues between staff and negative perceptions in the local community.
2. **Induction** – preparing people appropriately has a direct impact on how well and quickly staff settle into their new role, team life and the environment, thereby reducing the risk of security incidents.
3. **Office closure and contract termination** – a clear and transparent process on office closure and when contracts come to an end should be implemented some time before the notice period begins. Failure to do so can have serious security implications.
4. **Stress management** – risky and high-pressured situations are more likely to lead to a highly stressed workforce, which can impact behaviours, relationships and the ability to make good security-related decisions.
5. **Employment policy and practice** – employees are more likely to feel valued and protected when employment policies (e.g. reward, performance and conduct) are clear and consistently applied. Disgruntled and dissatisfied staff are a source of security threats to the organisation, staff and programmes.

Whilst reading this module, it is worth noting:

- The employee should have the competence and tools to do the role well.
- The working environment should be one where an employee feels healthy and safe.
- Employees should know their health, safety and security responsibilities, understand the risks, and accept any residual risk they face when undertaking their role, knowing that there has been appropriate analysis and care taken by the organisation.
- Employees should have the option to say no if they are concerned about the risks they are being asked to take to carry out their role.

The employee cycle and good people management

Ensuring your people management standards remain high and meet your duty of care obligations involves everybody in the organisation, starting with the most senior, and including every level of staff.

The employee cycle is a good way to identify the practices in people management which carry an obligation or risk. The best solution for good people management integrates security risk management with all stages of the employee cycle.

Using the employee cycle can also assist in understanding who owns or is responsible for the different practices in the organisation. In most cases, there is more than one person involved or a body or group that is responsible e.g. a risk management group (sometimes known as a health and safety committee).

Governance

The first stage of the employee cycle is governance, i.e. the structures and policies that your organisation is built upon. An organisation's health, safety and security culture relies heavily on having robust systems and practices in place. The key ones are often the basic ones. Employees are more likely to feel valued when policy and practice are clear and applied consistently. If practice is poorly aligned, or poorly implemented, this will adversely impact your employees and increase the risk to their health, safety and security. Key practices and the minimum levels of provision for each are outlined below.

Robust practices are ones which are value-centred, of a high standard, sustainable, accessible, relevant, known, used, monitored and evaluated.

Practice	Minimum levels of provision
Mission, goals, values	Clarity on the mission, goals and values provides vision and clear expectations. The mission demonstrates why the organisation exists and how it would like to change the world for the better. The mission is needed to motivate staff. The goals ensure that employees are working towards the same purpose. The values show how the organisation will do its work and the kinds of employees needed to do it. Everything should come back to this: the big picture.
Organisational risk threshold	The risk threshold identifies what the board/senior management of an organisation considers to be an acceptable level of risk for the organisation. The threshold may be different for different types of activities (e.g. saving lives vs. development). The risk threshold forms the basis for all security risk management policies and plans throughout the organisation. It also enables individual staff to check their own acceptable risk threshold against that of the organisation.
Organisational strategy and structure	A strategy gives direction by providing a picture of the work to be done, by whom, where and by when. The organisational structure outlines who is who in the organisation. It is used for job descriptions, grading and job titles, and shows the numbers for reporting lines. It aids recruitment, induction and general management and communication across the organisation.
Contract of employment and employee handbook	Legal, clear and accessible contracts and handbooks with consistent principles of employment practice are required for all defined categories of staff, including short-term contracts often used during an early humanitarian response stage. For local contracts, make sure to seek local legal advice. The employee handbook is a reference tool for managers and employees that contains useful information about the organisation, the terms and conditions of employment, and outlines the organisation's policies.

Practice	Minimum levels of provision
Pay and benefits	Pay and benefits (including allowances) should be applied using consistent principles, aligned with local practice and adaptable for an early humanitarian response stage. Employees should be consulted on changes to their pay and benefits. Variations for different staff types – international, re-located, national, volunteer, etc. – must be clearly defined. Actions concerning benefits include: **Leave** – monitor annual leave and carryover, national holidays, rest and recuperation (R&R), sick leave and maternity/paternity leave. Support sickness absences appropriately and conduct 'return to work' meetings. **Retirement** – provide details of an optional retirement scheme. **Insurance** – provide a summary of medical, travel and death in service provision with annual reviews and records of cases.
Working hours	Working hours and compensation for overtime, with adaptable working patterns for when staff initially respond to a sudden onset emergency.

Security implications

Humanitarian organisations should aim to link their values to the core humanitarian principles. These principles, particularly those of neutrality and impartiality, can help organisations gain local acceptance and safe access to insecure environments. Employees who do not follow these principles or their organisation's values can place themselves and the organisation at risk.

A weak organisational structure can result in a lack of clarity on where security responsibility lies within the organisation, including what the decision-making structure is during a critical incident, e.g. a staff abduction.

Transparency on grade, pay and allowances for all categories of staff reduces concerns and complaints. A lack of clarity on contractual stipulations, e.g. early termination, can lead to disgruntled employees retaliating and compromising the security of other employees, the organisation and programmes. Clear disciplinary procedures must be in place to deal with employees who pose a threat to their colleagues.

Recruitment

Risky environments require employees with specific skills and experience. An organisation should never underestimate the importance of the recruitment process and the risks associated with hiring the wrong person. Recruiting the wrong person can be very costly and unproductive, and employees who do not fit the role are likely to be unhappy and underperform, which will have a direct impact on programme implementation, their manager's time, team morale and security. A risk assessment of the role should be completed before the recruitment process starts, to understand the essential requirements of the role, and to ensure that suitable candidates are encouraged to apply.

Managers should be fully immersed in the recruitment of their teams.

Identifying a candidate's strengths and areas for development, and assessing them against essential values, skills and competencies is a crucial part of the process. The manager, in liaison with human resources and security, should undertake risk assessments to determine the risks that need mitigating for the particular applicant in the specific role. For high-risk roles or roles in high-risk contexts, mandatory health and safety interventions should be identified. The recruitment process should inform the content of an induction.

See Module 3 – Risk assessment tool

Practice	Minimum levels of provision
Recruitment	A clear job description and well-managed recruitment process using competency-based techniques with diversity at the heart. References and background checks are verified, and risk assessments are undertaken both for the role and the applicant, including health and resilience assessments. Managers are fully trained in the recruitment process. Where the manager does not speak the local language, steps must be taken to ensure that job applicants are not 'pre-screened' by local staff to avoid the risk that one section of the local community is given an unfair advantage.
Equality and diversity	An equality and diversity policy must be in place and employees should understand its principles and apply them in their work and behaviour. Discrimination characteristics should be outlined and strong sanctions set in place for any breach of policy. While discrimination in recruitment based on ethnicity, gender or sexuality is morally and legally unacceptable, in many environments the ability of an organisation to operate may be affected by the characteristics of an individual and these risks must be considered as part of the role risk assessment.

Security implications

The manager, in liaison with security and human resources, must carry out a robust risk assessment for all roles during the recruitment phase; this is in order to understand the risks inherent in the role itself and to help identify the type of candidates that should be recruited.

Once applicants have been identified, a risk assessment for the individual in the specific role should be completed. This is to assess the impact their skills, experience, age, gender, sexual identity, disability or ethnicity could have on their personal safety and security, whilst at the same time ensuring compliance with equal opportunity legislation.

Ethnicity, in particular, of both national and international staff, may have serious implications for the perception of your organisation and the risks both individuals and the organisation face.

The manager's aim is to recruit the most qualified person and ensure mitigating measures are in place to enable the individual to work in an environment with the lowest security risk possible. Understanding the diversity of your staff will help you develop better security systems and confidential, accessible resources to support their safety.

It is extremely important to dedicate time to verifying background checks and references for new recruits during the recruitment phase, especially for organisations that work with vulnerable people, e.g. children, and where a breach of the code of conduct can result in serious reputational and security risks for the employee and the organisation.

Induction

Preparing an employee for their assignment is one of the single most important things an organisation can do. It is not reasonable to send an employee to a high-risk environment without substantial preparation. Leaving an ill-equipped employee to make decisions that could jeopardise their personal security (and the security of others) is an abdication of responsibility and duty of care. Three areas, in particular, require attention:

1. Employees should be informed of the organisational security policies and procedures:
   - They should understand the acceptable level of risk for the organisation, and the policies which govern the security culture.
   - They should have confidence in the organisation's systems to manage their safety, security and well-being.

2. Employees must be aware of the risks to their own personal security:

- They should fully understand the context in which they are working (how the society around them functions and communicates) and how their own behaviour can affect their vulnerability.
- They should know what is expected of them (e.g. mitigation measures) during and outside normal working hours, and should behave accordingly.

3. Staff should be aware of how stress affects their personal behaviour:

- People can often release stress in damaging ways, such as excessive drinking and promiscuity.
- Organisations must provide the learning ground for managers and employees to be aware of and to manage their stress, and consistently enforce sanctions against employees who put themselves and others at risk.

Practice	Minimum levels of provision
Induction	An induction programme, led by the manager for each employee, includes information and training on: the mission, goals, behaviours, structure and reporting lines; strategy; team/ programme mandate; key relationships; the role; handover; contextual health, safety and security; probation objectives; key policy and practice.
Informed consent	Informed consent means: the staff member has agreed and signed a document which states that the security risks that come with the role and context have been fully explained, and the staff member has understood them; they understand the provisions the organisation is making to manage the risks in the context; they understand what is expected of them; and they are comfortable with the residual risk that remains after the organisation has put in place mitigating measures. The informed consent process should also include discussion of individual vulnerabilities.

Informed consent is a process to ensure staff engagement and understanding – it is NOT a legal waiver.

Security implications

An ill-prepared employee can make erroneous security decisions that are based on a weak understanding of the local security context. Staff who have accepted a posting without being aware of operational or personal restrictions (such as an early evening curfew) are more likely to break security procedures, put themselves and their programme at risk, and be demotivated and dissatisfied with the organisation. This contributes to a higher staff turnover.

Handover and a good induction, with appropriate support from line management, is essential for all new employees, and even more so when the role carries responsibility for making decisions about staff health and safety in a high-risk environment. For example, one of the key areas of concern in a legal case heard in Norway in 2015 (Dennis vs Norwegian Refugee Council) was the newly appointed country director's lack of knowledge about the local security context.

Health, Safety and Security

The extent to which organisations see staff as central to their mission is often reflected in the policies and practices that relate to staff health, safety and wellbeing. The health and safety of employees is a prime responsibility of any organisation and must be managed appropriately at all levels. Employers must take all 'reasonable steps' to prevent 'reasonably foreseeable' physical and psychiatric injury to their employees.

Preparation for the role, including training on self-care, psychological first aid, hostile environment awareness, and security and stress management, goes a long way towards keeping employees fit and healthy and able to respond to a crisis or security incident. Training and capacity building should not be overlooked – they are a priority.

The key questions below will help you test the robustness of your organisation's health, safety and security policies and practices.

Health

- Are employees physically and mentally resilient enough to carry out their roles? Are they aware of their stress triggers?
- Does the organisation have critical incident procedures, along with a sexual violence policy, and a team qualified to respond to such incidents?
- Does the organisation offer a confidential advice service, with referral to appropriate counselling or treatment services?

Assumptions are often made about the mental resilience of employees. Experienced international employees are often the first choice for high-risk postings. Do you continually assess their levels of resilience and know how to support them appropriately? It is also important to remember that employees from the local community are as likely to be traumatised by severe events as any other members of the local population they are helping.

▶ *See Module 12 – Medical support and evacuation*

Safety

- Has a health and safety assessment been carried out for each location and reviewed regularly?
- Are accidents reported and is medical support available, including psycho-social support?
- Are trained First Aiders present in the office, and are staff aware of how to contact them?

An employer must make the place of work as safe as possible and provide a safe system of work. If a place of work becomes temporarily unsafe, the employer must consider taking further reasonable steps to reduce the danger, including the possibility of ceasing the work activity altogether.

- *See Module 10 – Travel safety: airports, vehicles and other means of transport*
- *See EISF guide 'Office Opening: A guide for non-governmental organisations'*
- *See EISF guide 'Office Closure'*

Security

- Does the organisation have a security risk management framework and local security plan in place to identify, mitigate and manage security risks, as well as respond to security incidents if they occur?
- Does your organisation have a positive culture of security, i.e. do all staff understand and commit to following security guidance in order to keep themselves, their colleagues and their operations safe?

- *See Module 1 – Security risk management planning process*
- *See Module 7 – Security plan*

Practice	Minimum levels of provision
Health, safety and security	Policy and training on staying healthy, safe and secure should be in place for each location and closely aligned with stress management, personal resilience, physical and psychological health, and security risk management practices. Clear reporting of accidents, illnesses or critical incidents is key. Managers are trained to closely monitor the health of their team, using supportive conversations, informal briefs and debriefs, and spotting early signs of stress to prevent cumulative stress and burnout within their team. For senior managers who are remotely managed, a system for peer support should be considered. The organisation should continually review its health and safety practices to ensure they are relevant and provide the appropriate staff safety measures. Key stakeholders should learn from situations that are a risk to staff, programming and the organisation.

Security implications

An individual's knowledge, behaviour and attitude impact their vulnerability and exposure to risk. The more employees understand why health, safety and security procedures are in place, the more likely it is that they will follow them. For example, staff are less likely to obtain recommended vaccinations if they do not know or understand the risks of falling ill while travelling.

Road traffic accidents are one of the most serious threats to aid worker safety in the field. Ensuring drivers are trained on how to drive safely and that travellers are wearing seatbelts can significantly reduce the likelihood and impact of road traffic accidents.

Staff responding to a humanitarian crisis, especially during a fast onset emergency, are more susceptible to high levels of stress due to working longer hours in a highly pressured environment. Putting in place measures to prevent and deal with staff stress, as well as training staff on how to identify and manage stress, improves the wellbeing of staff and their decision-making. Overworked and highly stressed individuals are more likely to make poor security decisions.

Any stress reduction measures, such as R&R, must be applied consistently, otherwise staff may feel peer pressure to ignore them, even when they are needed.

See EISF guide 'Security Audits'

Performance and Development

The ability to achieve the work set out in the organisation's strategy is reliant on the employee being able to do their role in a healthy, safe and secure way. Adequate supervision and instruction must be provided to employees. Setting clear expectations with a focus on impact and providing the necessary support will help employees succeed. Through frequent two-way communication, formal and informal, the manager can listen to staff concerns and determine if performance is good and, if not, use relevant policy and practice in a consistent way to manage poor performance, grievances and misconduct.

Can't versus won't: poor performance is managed in either of two ways – a capability policy is used when the employee does not have the skills or competencies to do the work; the disciplinary policy is used when the employee will not do the work.

The frequent communication between the manager and employee should include conversations about personal development for their current and future roles. Actively supporting employees in their current activities and their career goals is more likely to motivate and enhance performance and effectiveness.

Practice	Minimum levels of provision
Performance management	Adequate supervision and instruction must be provided. Job descriptions and objectives must be clear. Frequent manager communication and feedback should take place with good performance rewarded and poor performance managed through either capability or disciplinary policies. Monitoring of security risk management should be specifically included in the performance review process for all staff who have any security responsibilities.
Grievance and disciplinary procedures	A trusted channel to raise informal and formal concerns and complaints should be in place. Grievance and discipline policy outlines a fair and consistent way to manage, monitor and learn from cases.
Whistleblowing	Whistleblowing is an anonymous way to raise a serious complaint or concern and for legitimate cases to be investigated in a confidential way.
Learning and development for the employee	Regular discussions on behaviours, development and career goals should take place.

Security should be part of every employee's performance review process.

Security implications

One of the greatest threats organisations face is from disgruntled staff. Employees who feel they have been unfairly treated can respond in a number of ways: theft, physical and verbal abuse, death threats, and 'bad-mouthing' individuals or the organisation to external stakeholders such as beneficiaries, elders and government officials, and to the media. These reactions can have serious security implications for staff, programmes and the organisation.

Performance management relies on a good employee-manager relationship. A poor relationship can erode trust and have serious implications for security if, for example, a manager's security recommendations are ignored or if an employee makes decisions which could place them and their colleagues at risk, without consulting their manager.

Without a trusted channel for raising concerns, employees may feel compelled to accept all decisions made by their managers, even if they are uncomfortable with the risks involved. Frontline staff are likely to have a better understanding of the security context but a lack of communication channels can impede information-sharing up the management line and increase the risk of a security incident occurring.

Transition

All employees leave an organisation at some point. The way an employee leaves can have an impact on the wellbeing of the individual, their colleagues and the reputation of the organisation. An employee who 'leaves well' can become an ambassador for the organisation. The more time and information an individual has to prepare for their departure, the better. Where possible, managers should start the discussions about departure before the notice period begins. It is also important to understand the reasons why staff choose to leave of their own accord.

See EISF guide 'Office Closure'

Practice	Minimum levels of provision
Pre-departure actions	Clear and transparent discussions with staff, particularly national staff, on the future of the project or office can enable employees to be better prepared for the transition and ensure that good handovers take place. Organisations should put in place measures to support staff transition, especially when the organisation is obliged to let staff go due to loss of funding or for other reasons outside of the organisation's control.
Exit interviews	Collect information and knowledge from leavers. Include questions on work-life balance, values, development, quality of briefings/debriefings and reasons for leaving. Multiple leavers from one team can indicate something more serious, and action must be taken.
Organisational learning	Learning from a leaver is a good way for an organisation to develop and manage its institutional knowledge.

Security implications

Unhappy leavers carry a security risk. Dismissals through disciplinary procedures, loss of funding, office closure and heightened security can all lead to different kinds of risks.

Disgruntled employees can disrupt project performance and relationships, and create a very unhealthy environment. In a high-risk environment, managing an employee's exit in difficult circumstances is one of the most important and complicated things a manager may have to do.

Sharing information with other employers, allowing more flexible working for job hunting and offering training opportunities (e.g. computer and English language skills) can aid staff to transition well and thereby reduce security risks.

If information is not collected from a departing employee (usually via a handover and through exit interviews), it is likely the learning will not be passed on and mistakes will be repeated. Without a good handover, there is a greater risk that a new employee will fail in their tasks and be a risk to their own and others' health, safety and security.

In order to learn and adapt, organisations need to carry out regular security assessments and apply what they learn. Crisis management exercises are also key for senior management.

When an unsuccessful programme was closing its office in Indonesia, it did not let its employees know until two days before the end of their contracts. Rumours had already circulated and employees were very upset. An office robbery took place the night before the final pay day to steal cash from the safe and take valuable items from the office. The managers believed it was best not to let employees know the exact closure date in the interests of security. However, the lack of transparency resulted in a more aggressive retaliation and compromised the security of staff. A more honest and supportive approach for the programme staff would have likely resulted in fewer incidents and greater security.

Where to read more

The CHS Alliance website (www.chsalliance.org) hosts resources which support organisations with the health, safety and wellbeing of their employees. Standard 8 of the 'Core Humanitarian Standard' outlines policies that should be in place for the security and wellbeing of staff.

Duty of Care International (http://dutyofcareinternational.co.uk/) hosts several resources including:

- The 'Human Resource Management (Roots 12)' guide published by Tearfund. This is a useful people management tool for managers, particularly where there is no human resource expertise in country.
- 'The Importance of HR Management in Supporting Staff Working in Hazardous Environments' by Roger Darby and Christine Williamson.
- 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff' by Edward Kemp and Maarten Merkelbach.

International SOS Foundation (www.internationalsosfoundation.org) provides a number of useful resources, including 'Managing the safety, health and security of mobile workers: an occupational safety and health practitioner's guide' produced jointly by International SOS Foundation and IOSH.

The EISF website (www.eisf.eu) hosts a number of relevant EISF publications that support organisations with staff care, as well as a library of further resources on staff health, safety and security.

Glossary

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

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

Digital Security: Measures, strategies and processes that aim to mitigate risks related to the use of technologies and individuals' and/or organisations' digital presence.

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

Hibernation: Staff stays at home and there is a temporary halt to programming during a crisis period. In some circumstances, staff may be required to shelter in the office or compound.

Protection: Reducing the risk, but not the threat by reducing the vulnerability of the organisation (e.g. fences, guards, walls).

Relocation: Shifting offices and/or activities from an unsafe area to a safer location, usually on a temporary basis and within the same country.

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

Evacuation: Suspending operations in a country, evacuating internationals to another state and national staff from deployed areas to their home areas. Some limited programming may continue using remote management, depending on the situation.

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

Trigger: Factors agreed between in-country staff and headquarters to determine when the various contingency plans should be activated.

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, its staff and ability to manage risks.

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
December 2016
Vazquez Llorente, R. et 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. and Margolies, E.

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

Abduction and Kidnap Risk Management
November 2017
EISF

Security Incident Information Management Handbook
September 2017
Insecurity Insight, Redr UK, EISF

Security Risk Management: a basic guide for smaller NGOs
June 2017
Bickley, S.

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 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 September 2015 / Updated March 2020

Design and artwork: www.wave.coop