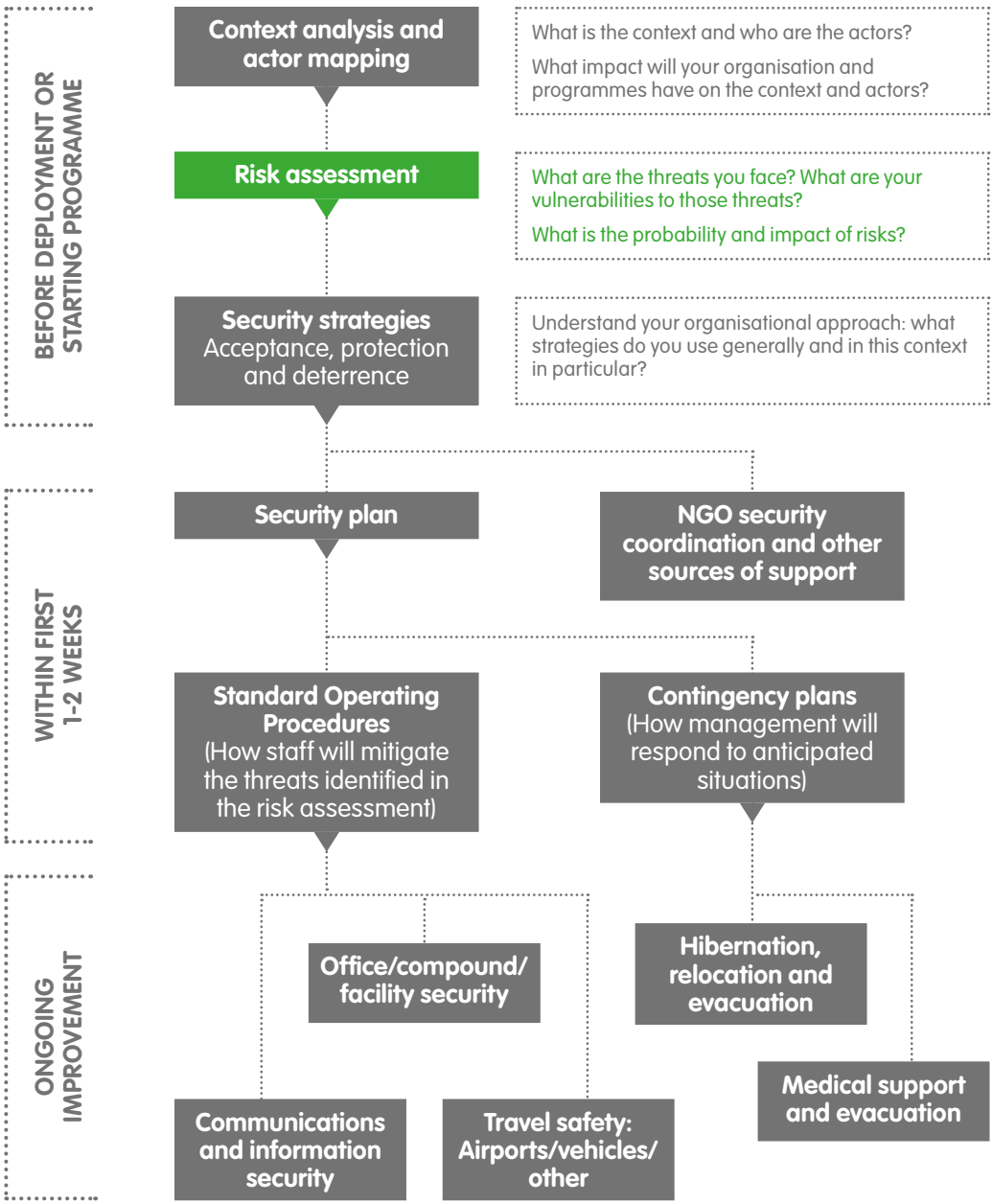
# 3 Risk assessment tool





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<br>National staff<br>Community members<br>Marked vehicles<br>Aid supplies | Loss of life<br>Loss of assets<br>Damage to reputation in community/with government<br>Reduction in ability to work |
| **e.g.** | Carjacking | Route to airport – Highway 1 | All staff<br>Marked vehicles<br>SUV | Loss of assets<br>Reduction in mobility of teams<br>Reduction in ability to work<br>Physical injuries to all staff<br>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<br>• Minimal loss or damage to assets<br>• No delays to programmes | • Minor injuries<br>• Some loss or damage to assets<br>• Some delays to programmes | • Non life-threatening injury<br>• High stress<br>• Loss or damage to assets<br>• Some programme delays and disruptions | • Serious injury<br>• Major destruction of assets<br>• Severe disruption to programmes | • Death or severe injury<br>• Complete destruction or total loss of assets<br>• 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.

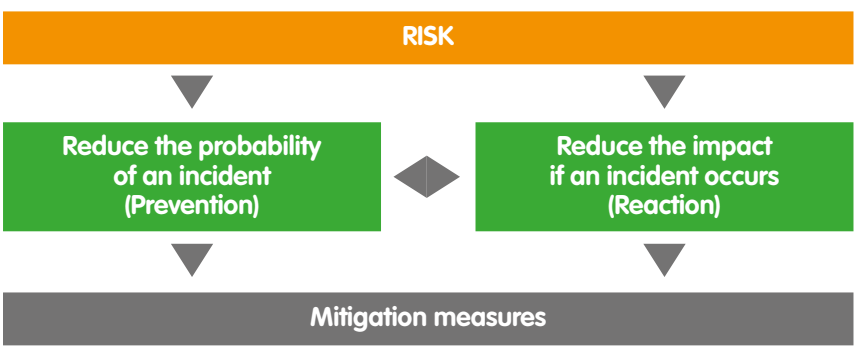
**Developing security strategies is a critical step in ensuring that before committing staff, resources and the organisation's reputation to a response, the agency has taken all reasonable steps to minimise the risk.**

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 4 – 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'*

# Contents

## European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 75 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

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

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

**www.eisf.eu**


## Acknowledgements

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

The European Interagency Security Forum (EISF) and James Davis would like to thank the working group 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 and William Carter.


## Suggested citation

Davis, J. (2015) *Security to go: a risk management toolkit for humanitarian aid agencies*. European Interagency Security Forum (EISF).


### Disclaimer

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

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

© 2015 European Interagency Security Forum



Design and artwork : www.wave.coop