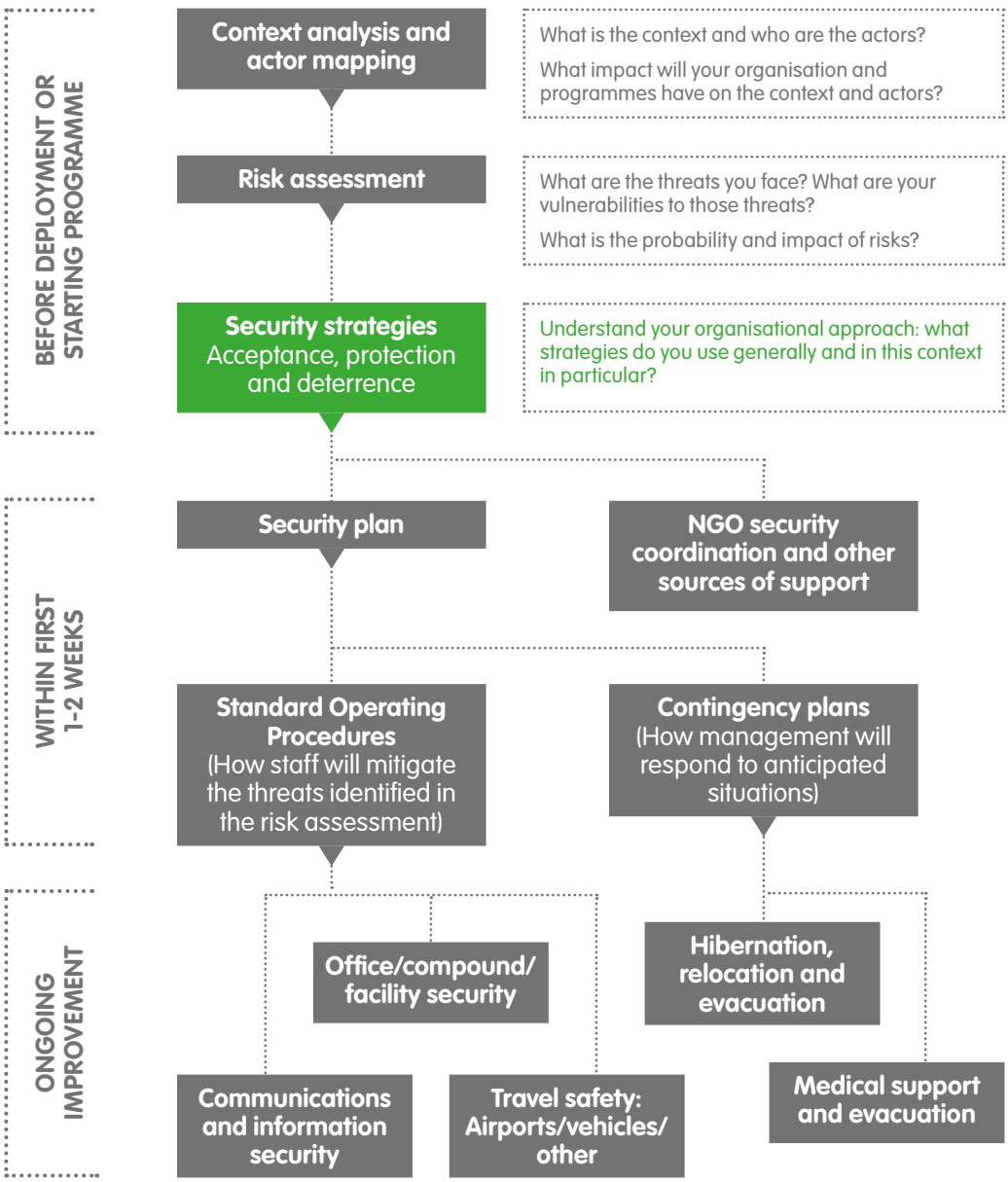
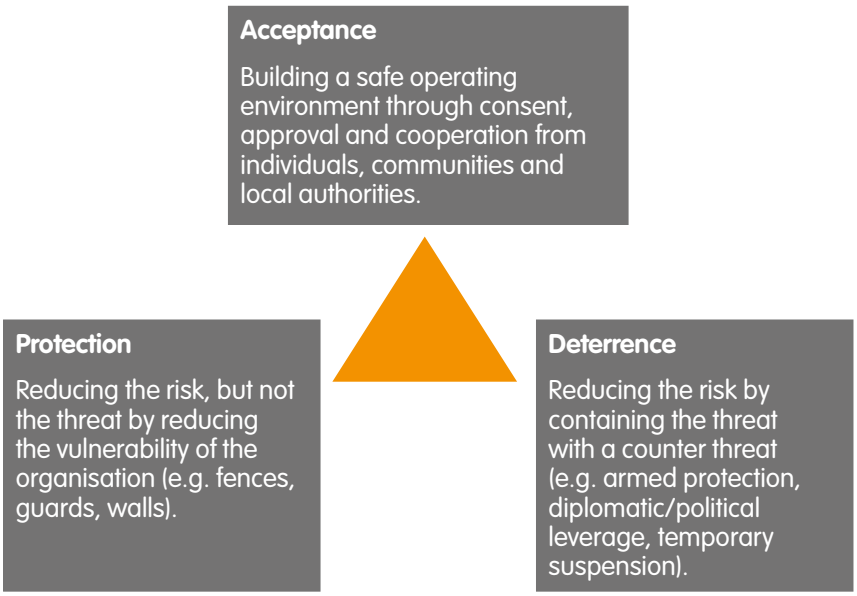
4 Security strategies: acceptance, protection and deterrence



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 5 – 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 7 – 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 8 – 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.

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).

Design and artwork : www.wave.coop