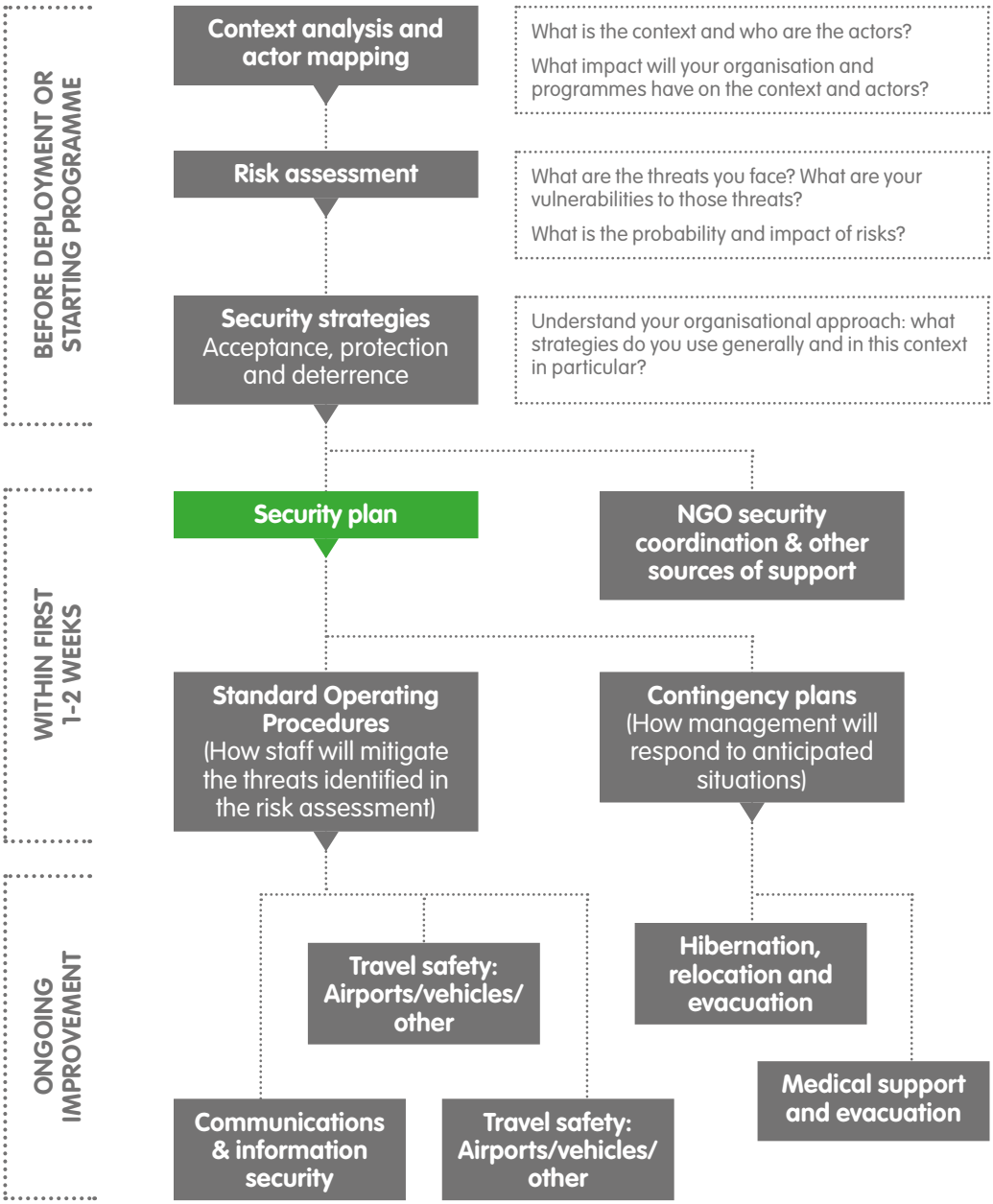
6 Security plan



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 4 – 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 9 – 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 10 – Hibernation, relocation and evacuation

See Module 11 – Medical support and evacuation

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