

1

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

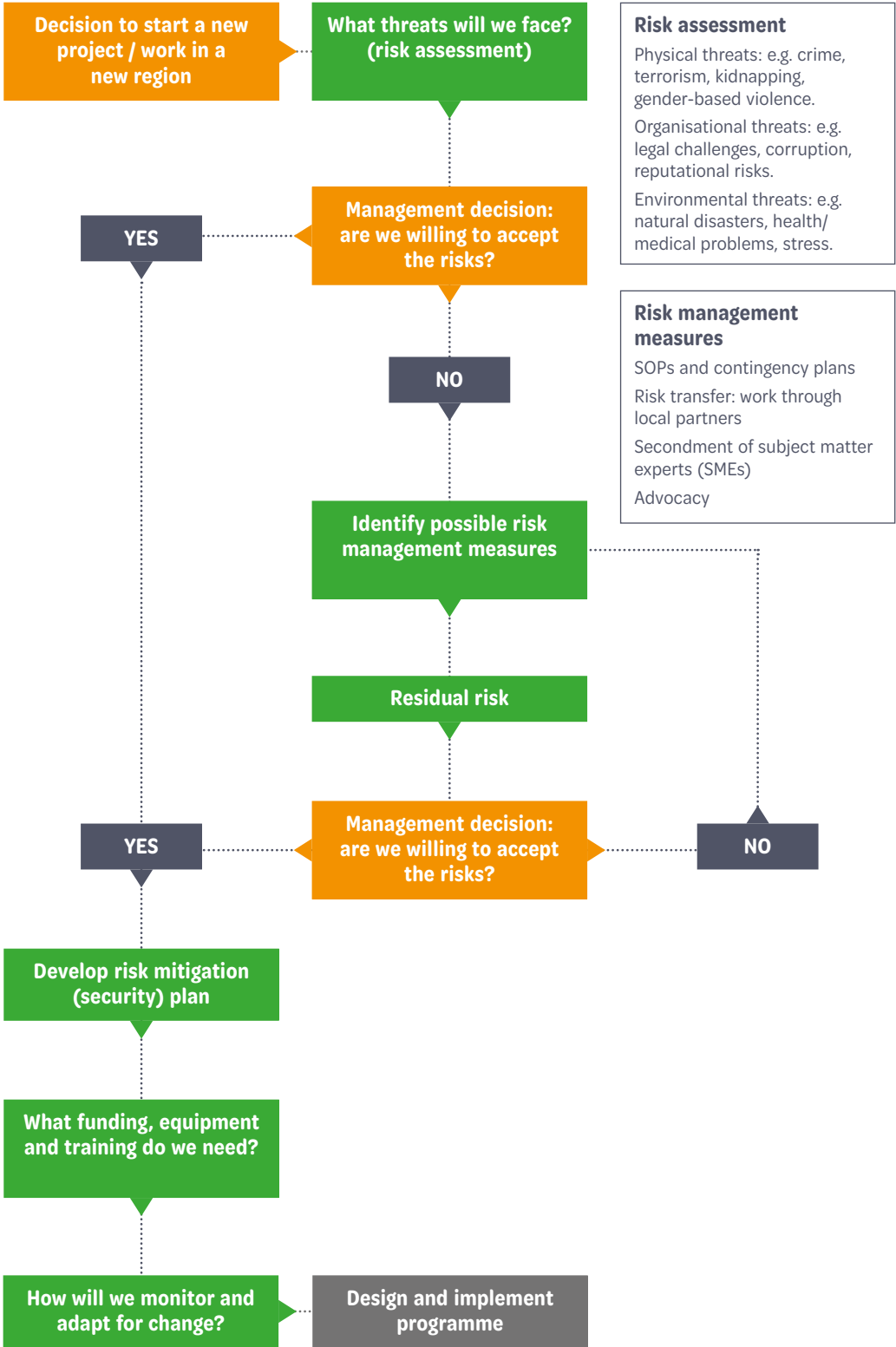
▶ See Glossary

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.



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.

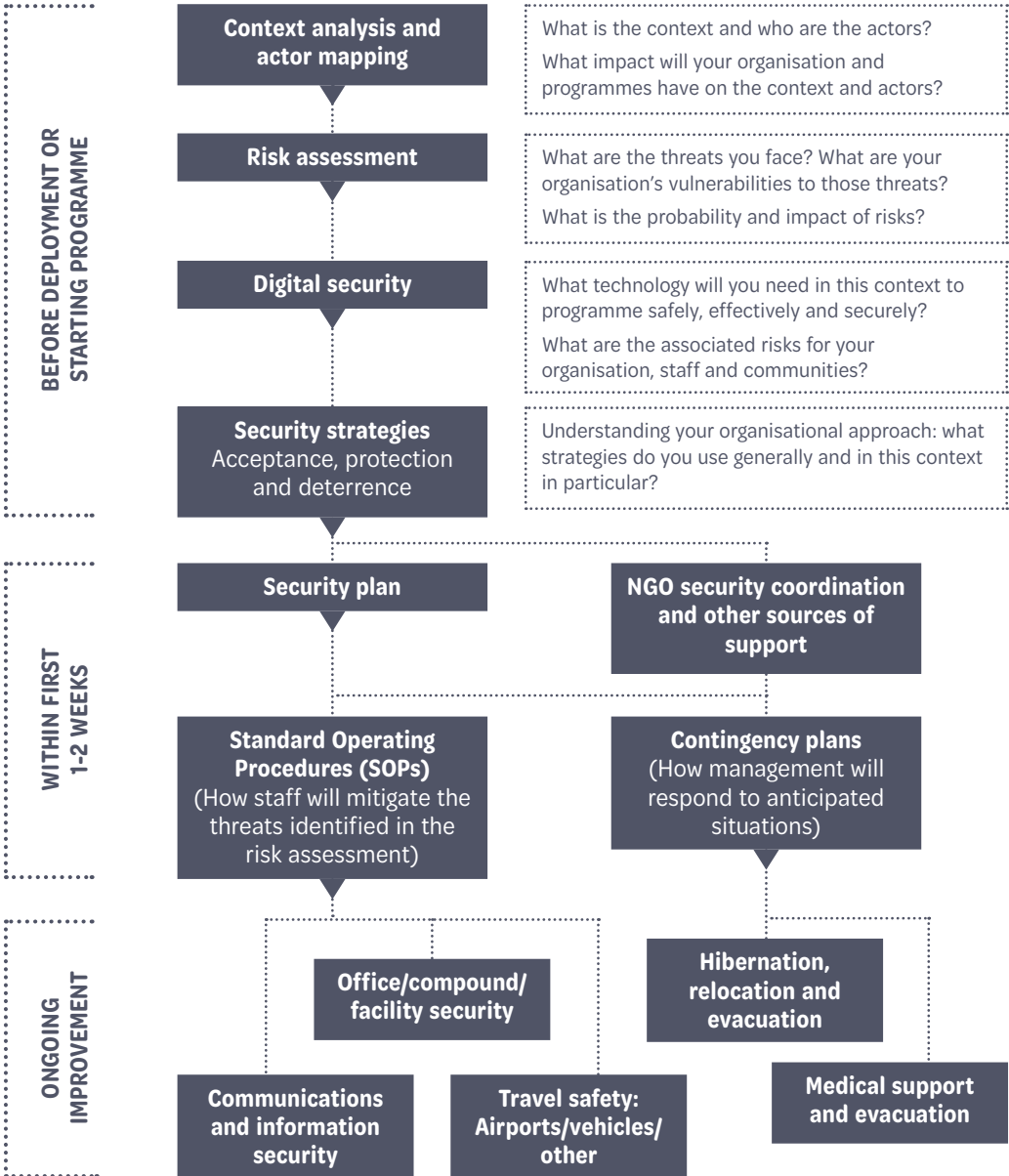
► *See Glossary*

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 GISF 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).