GUIDANCE

Security risk management: a basic guide for smaller NGOs

What a small organisation can actually put in place, in what order, and with what resources, when it has no security manager and no security budget line.

European Interagency Security Forum

Almost all guidance on security risk management is written for organisations that have a security function. Most humanitarian organisations do not. They have a director who also manages programmes, a finance officer who also manages human resources, and a field team that is expected to look after itself. Advice that assumes a security manager, a dedicated budget and an annual assessment cycle is advice that cannot be used, and the gap it leaves is filled by nothing.

This guide is written for the organisation with fewer than fifty staff, no security specialist and a genuine exposure to risk. Everything in it can be done by somebody who already has another job.

The order of work

Five things, in this order. Each is a precondition for the next, and the order is what makes the list achievable.

Step	What it is	Who does it	Time
1	Name one person as the security focal point, with the authority to act	The director	An afternoon
2	Write a one-page security plan for each location where you have staff	The focal point with the field team	Two days per location
3	Build the communications tree and test it	The focal point	One day, then twice a year
4	Brief every member of staff on the plan, and record that you did	Line managers	Two hours per person
5	Put a figure in the budget for security, and spend it	The director and the board	One budget cycle

Steps one to four cost almost nothing. Step five is the one that decides whether the rest is real, because an organisation that has never had a security budget line will not acquire one by having a better plan.

The one-page security plan

A plan that fits on one page gets read, updated and used. A plan of forty pages, produced by a consultant, is filed and never opened. The one page carries the following.

- ☐ **Who is in charge** in each location, by name, with a deputy, and the limits of what they can decide without calling the director.
- ☐ **The threats that matter here,** in plain language, no more than five.
- ☐ **The rules that apply to everyone:** movement, check-in, curfew, communications, vehicles.
- ☐ **What to do in the first ten minutes** of each of the four incidents most likely to occur. Not a procedure, a sequence.
- ☐ **The phone numbers** that matter, including the ones that answer at night.
- ☐ **The medical arrangements,** including the nearest facility that can actually treat a serious injury and how a person gets there at night.
- ☐ **The trigger for leaving,** stated as a condition rather than as a judgement: what has to happen for the team to relocate or withdraw.
- ☐ **The date it was written, and the date it will be looked at again.**

The communications tree

The single most useful arrangement a small organisation can make, and the one most frequently documented and never tested.

- **Direction.** Who calls whom, in what order, for two scenarios: an incident involving one member of staff, and an incident affecting the whole team or the location.
- **Fallback.** A second route when the first does not answer, and a rule about how long to wait before using it.
- **Escalation.** The point at which the director is called, stated as a time or a condition rather than as a judgement.
- **Outward.** Who calls the family, who calls the donor, who speaks to anybody external, and the rule that nobody else does.
- **Test it.** Twice a year, unannounced, and record how long it took and where it broke. A tree that has never been tested is a diagram.

What a small organisation genuinely cannot do, and what to do instead

Cannot	Instead
Employ a security manager	Name a focal point with a written role description, give them training, and give them time. One trained person with authority is worth more than a committee
Run its own analysis	Use the coordination mechanisms in the country, buy a commercial report if the budget allows, and rely on the network of peer organisations. Reciprocity is the currency, so contribute what you see
Train staff in house	Buy one external course for the focal point and require them to brief everybody else. Briefings delivered by a colleague are better attended than courses delivered by a stranger
Provide its own crisis response	Establish what the insurer provides before you need it, and check that the assistance line works from the countries you operate in. Most organisations discover the limits during an incident
Insure at the level of a large agency	Check the cover against the postings rather than against the contract type, and tell each person in writing what is and is not covered. A documented gap is survivable; an undocumented one is not
Evacuate without help	Agree in advance, in writing, who will help: a larger agency, a partner, the coordinating body, the embassy. An agreement made during an evacuation is not an agreement

The partner question

Small organisations frequently work through local partners, and the arrangement is where the exposure concentrates. The partner delivers the programme, employs the staff who are actually exposed, and usually has fewer resources than the international organisation that commissioned the work.

Three requirements, all of them cheap. Fund the partner to manage security rather than requiring them to absorb the cost of an international organisation's presence. Agree in writing what happens if a partner's staff member is harmed while delivering your programme, including who pays and who speaks to the family. And include the partner's staff in your briefings and in your communications tree, because an incident involving them is an incident involving you.

The board's part

A small organisation's security practice is set by its board, whether or not the board discusses it. Three things are being asked of it. Approve a security budget line. Ask, once a year, what the organisation's principal risks are and what was done about them. And accept in writing the residual risks that the organisation has decided to carry, so that the decision has an owner.

Published by the European Interagency Security Forum as part of its resource library.

This guide is published for information and training purposes. It is not legal advice. Organisations should check their obligations under the law of the jurisdictions in which they employ and deploy staff, which may require more than this guide describes.