HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

Mini MBA Security and Risk Management: protecting teams and maintaining access

Course handout · Week 11 : Sharing risk with partners and funding security

A programme of exactly 3 months (12 weeks, 144 hours) to manage the security and risks of a humanitarian organisation: duty of care, context analysis, risk assessment, plans and procedures, acceptance and access negotiation, incidents, crisis management and kidnapping, staff health and wellbeing, digital security and data protection, organisational risks and compliance, risk sharing with partners, governance and business continuity. Corrected numerical exercises, three monthly exams with case studies, and a verifiable diploma from the Humanitarian Academy.

https://humanitairejobs.org/en/academy/mini-mba-securite-risques/semaine-11/

Free document from the Humanitarian Academy. It may be printed and shared freely for training purposes, without modification.

Week 11 : Sharing risk with partners and funding security

Objectives

- Analyse the transfer of risk to national and local partners and build equitable risk sharing.
- Budget for security comprehensively and defend it to donors.
- Organise security in consortia, remote management and inter-agency coordination.

Risk transfer

When access becomes difficult, international organisations increasingly rely on **national and local partners**, who are better accepted and often the only ones present. This is a strength for the response and for localisation, but it can turn into **risk transfer**: the international organisation reduces its exposure by exposing the partner more, without giving it the means to cope.

Signs of unfair transfer:

- the partner works in areas where the international organisation forbids its own staff to go, without a joint risk assessment;
- the partner's budget contains no security line (communications, insurance, training, suitable vehicles);
- the partner bears the fiduciary risk alone (losses and thefts reimbursed by the partner) as well as the legal risk (sanctions);
- no assistance is planned in the event of a serious incident affecting the partner's staff.

Towards equitable sharing

Risk sharing is an approach that recognises that risks must be allocated according to each party's capacity to manage them, and funded. Inter-agency work on this subject (notably within the framework of the Grand Bargain and NGO networks) proposes:

- a **joint assessment** of risks with the partner, before the agreement;
- **eligible security costs** in the partner's budget, matching real needs;
- partner access to **training**, security analyses and emergency arrangements (medical evacuation, insurance);
- a clear sharing of **fiduciary risk**: which losses are accepted if procedures were followed, and which are reimbursed;
- **mutual commitments** in the event of a serious incident: assistance, communication, support to families.

> A test question: if this incident happened to our own staff, what would we do? Does the partner deserve less?

Budgeting for security

Security costs money, and its costs must appear clearly in budgets; otherwise they are taken from elsewhere or ignored. Typical budget lines:

- **Staff**: security adviser, focal points, guards, radio operators.
- **Equipment**: communications (radios, satellite phones, trackers), suitable vehicles, site protection, personal protective equipment depending on the context.
- **Training**: basic security, advanced training, first aid, crisis exercises.
- **Services**: subscriptions to analysis services, security forums, medical evacuation, specific insurance.
- **Contingency reserves**: hibernation, relocation, evacuation.

Example of a country's annual budget (USD 8 million of programmes, 150 staff). Security adviser and 3 focal points: 140,000; guards (6 sites): 90,000; communications: 45,000; training and exercises: 35,000; site upgrades: 40,000; specific insurance and medical evacuation: 60,000; contingency: 30,000. Total: USD 440,000, i.e. 5.5% of programmes and about USD 2,933 per staff member. This percentage varies widely between contexts, often from 2 to 15%.

Defending the security budget

Donors generally accept security costs if they are **justified, proportionate and linked to access**. Effective arguments:

- link each cost to a risk identified in the risk assessment and to an activity;
- show what security makes possible: access to specific areas, continuity of activities, protection of the people assisted;
- present the costs as direct project costs (pro rata, according to justifiable allocation keys) rather than burying them in indirect costs;
- show the data: incidents avoided or better managed, days of activity maintained.

Example of a quantified argument. Last year, without satellite phones, the teams at two bases suspended their movements for a total of 45 days each time the mobile network went down. Equipping these bases costs USD 12,000; the 45 days of suspension delayed activities worth USD 300,000. The investment is small compared with the continuity it provides.

Consortia, remote management and coordination

In a consortium, each member remains responsible for its own staff, but the lead agency must ensure that risks are assessed and managed by all: joint assessment, information-sharing, common alert procedures, a security budget for each member.

In remote management, the security of the teams on the ground (national staff, partners) becomes the priority: local analysis by those who are exposed, the right to refuse an activity, communications, means of relocation, and regular contact.

Inter-agency coordination:

- **NGO security forums** (national platforms for sharing information and analysis, often funded by donors): alerts, incident reports, training, analyses.
- The **"Saving Lives Together"** framework, which organises cooperation between the United Nations security management system and partner NGOs.
- The **Global Interagency Security Forum** (GISF) at international level: guides, research, exchanges between security managers.

Information-sharing requires rules: confidentiality, anonymisation, prior agreement for any data that does not belong to the organisation.

Measuring risk management maturity

An organisation can assess its **maturity** in security risk management on a few dimensions, scored from 1 (non-existent) to 4 (integrated and continuously improved):

- policy and governance (risk threshold, responsibilities);
- up-to-date risk assessments and plans;
- training and skills;
- incidents and learning;
- crisis management;
- equitable duty of care (national staff, partners);
- resources and budget.

Example. An organisation's scores: 3, 2, 2, 1, 3, 1, 2. Average: 14 / 7 = 2. The two scores of 1 (incidents and learning; equitable duty of care) are the priorities: they concern the capacity to learn and equity, on which the other dimensions rest. An annual self-assessment, discussed by the board, makes it possible to track progress.

Exercise: a partner on the front line

Situation. Your organisation funds a local NGO for child protection activities in a province where your staff are no longer authorised to go. The partner's budget (USD 600,000) includes no security costs. The partner has 40 staff on site; two of them were detained for 3 days last month; it has neither accident insurance nor a satellite phone. The agreement provides that any loss of assets, even due to looting, is reimbursed by the partner.

Task. 1) Identify the problems. 2) Propose a realistic security budget for the partner (communications 6,000; training 8,000; accident insurance at 3% of a payroll of 240,000; contingency reserve 10,000; half-time security focal point 9,000). 3) What changes to the agreement?

Answer. 1) Unfair risk transfer: an area judged too dangerous for your staff, without a joint assessment; no security costs; detention with no support planned; fiduciary risk entirely transferred, including for force majeure. 2) Communications 6,000 + training 8,000 + insurance 7,200 + contingency 10,000 + focal point 9,000 = USD 40,200, i.e. 6.7% of the budget; to be funded additionally or through reallocation, with a justification to the donor. 3) Joint risk assessment and the partner's right to suspend a dangerous activity; a security budget line; access to your organisation's training, analyses and medical evacuation; a fiduciary risk-sharing clause (losses due to looting accepted if procedures were followed and the incident reported); a commitment to provide assistance in the event of detention or a serious incident.

Key takeaways

- Working with partners must not become an unfair transfer of risk.
- Risk sharing: joint assessment, security budget, access to training and arrangements, shared losses.
- Budget security as direct costs, linked to risks and activities, often 2 to 15% depending on the context.
- Defend security through the access and continuity it provides, backed by figures.
- NGO security forums, Saving Lives Together, GISF: coordination with confidentiality rules.

Quiz

1. Security budget USD 360,000 for USD 6,000,000 of programmes. Share:
   A. 3.6%
   B. 0.6%
   C. 16.7%
   D. 6%
2. Same budget for 120 staff. Cost per staff member:
   A. USD 300
   B. USD 50,000
   C. USD 3,000
   D. USD 30,000
3. A partner alone reimburses any loss due to looting, even if procedures were followed. This is:
   A. Equitable sharing
   B. An unfair transfer of fiduciary risk
   C. Good practice
   D. A requirement of all donors
4. Maturity scores of 2, 3, 1, 2, 2 on 5 dimensions. Average:
   A. 2
   B. 2.5
   C. 1.8
   D. 10
5. In a consortium, the security of each member's staff is the responsibility of:
   A. The lead agency alone
   B. The local authorities
   C. The donor
   D. Each member, with a system coordinated by the lead agency

Quiz answers : 1. D · 2. C · 3. B · 4. A · 5. D