HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

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

Course handout · Week 1 : Duty of care and security risk management: the framework

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-1/

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

Week 1 : Duty of care and security risk management: the framework

Objectives

- Explain the duty of care of a humanitarian organisation and its legal, ethical and operational consequences.
- Describe the security risk management cycle and the three strategies: acceptance, protection, deterrence.
- Position security in the service of access and programmes: staying and delivering, rather than running away or taking reckless risks.

Why security is a leadership function

Every year, hundreds of aid workers are killed, injured or kidnapped; the vast majority are **national staff**. Public databases on aid worker security show that violence is concentrated in a small number of contexts, but that no organisation working in a crisis zone is immune.

Security is not first and foremost about guards and walls. It is a **leadership function** that makes it possible to reach people in need while keeping risks to staff at an acceptable level. An organisation that manages its risks poorly loses its access, its teams, its funding and sometimes its reputation.

> The aim of security risk management: to enable sustainable access to populations, not to eliminate all risk. The only way to eliminate all risk is to do nothing.

Duty of care

Duty of care is the legal and moral obligation of an organisation to take all reasonable measures to protect its staff from foreseeable harm. It extends, to varying degrees, to consultants, volunteers, visitors and partners.

In practice, it requires the organisation:

- to **assess** risks before exposing anyone;
- to **inform** staff clearly about risks (informed consent);
- to **train** and equip;
- to put in place proportionate **measures** (procedures, communications, insurance, psychosocial support);
- to **respond** to incidents and learn.

Court rulings in several countries have recognised the liability of humanitarian organisations that had not taken reasonable measures in the face of a known risk. Duty of care cannot be

fully delegated: an organisation remains responsible even when it relies on a contractor or a shared mechanism.

It must be **equitable**: historically, national staff have received less training, equipment and evacuation options than international staff for an equal or higher risk. Current good practice requires this inequality to be addressed explicitly.

The security risk management cycle

The most widely used framework in the sector (formalised notably by Humanitarian Practice Network Good Practice Review 8 and the guides of the Global Interagency Security Forum, GISF) follows a cycle:

- **1. Context analysis**: actors, dynamics, trends in violence.
- **2. Risk assessment**: threats, vulnerabilities, likelihood, impact.
- **3. Choice of strategies and measures**: acceptance, protection, deterrence.
- **4. Plans and procedures**: security plan, standard operating procedures, contingency plans.
- **5. Implementation**: training, equipment, budget, responsibilities.
- **6. Monitoring, incidents and review**: reporting, analysis, regular updating.

The cycle runs continuously: any significant change in the context (elections, military offensive, serious incident) triggers a review, without waiting for the scheduled date.

Acceptance, protection, deterrence

Three strategies are combined, in a mix specific to each context:

- **Acceptance**: obtaining the consent of communities, authorities and parties to the conflict for the organisation's presence and activities, through relevant programmes, respect for principles, dialogue and staff behaviour. It is the core strategy of humanitarian organisations.
- **Protection**: reducing vulnerability through measures and equipment (movement procedures, walls, unarmed guards, communications, suitable vehicles, shelters). It protects but can distance the organisation from communities ("bunkerisation").
- **Deterrence**: posing a counter-threat to deter aggression (armed guards, armed escorts, conditional suspension of activities). It is reserved for exceptional cases because it can compromise neutrality and acceptance.

Example. In an area where the organisation is well accepted but urban crime is high, the typical combination is: acceptance in the communities served, reinforced protection of residences and movements in town (no walking at night, locked vehicles), and suspension of activities as a deterrence lever in the event of a targeted attack.

The acceptable risk threshold and programme criticality

All exposure must be **justified by the value of the programme**. The higher the risk, the more critical the activity must be for people (saving lives) and the more the organisation must genuinely have the means to manage it.

Programme criticality tools (for example the United Nations framework) rank activities from the most critical (immediate life-saving activity, or one directed by the Secretary-General) to the least critical. A low-criticality activity does not justify a high risk; a life-saving activity can justify a high risk, but not an unacceptable risk.

Decision example. A three-day project management training course in a city where the risk of kidnapping is assessed as high can be moved or delivered online. A vaccination campaign against an epidemic in the same city can be maintained with reinforced measures, because the life-saving benefit justifies a higher residual risk, within the limit set by senior management.

> The acceptable risk threshold is set by the organisation's senior management, in writing, and not by the bravest team in the field.

Roles and responsibilities

Security is everyone's business, but responsibilities must be clear:

- **Board and executive management**: security policy, acceptable risk threshold, resources, oversight of serious incidents.
- **Country director**: responsible for security in the country; this is a leadership role that cannot be fully delegated to the security adviser.
- **Security manager or adviser**: analysis, advice, procedures, training, incident follow-up.
- **Security focal points** in field bases.
- **Every staff member**: follow procedures, report, behave in a way that protects acceptance, and say no to a mission judged too dangerous.

The **right to withdraw**: anyone may refuse to go to a location or may leave a location if they consider the risk too high, without sanction. Conversely, management can prohibit a trip even if the person volunteers.

Exercise: a country director faced with a mission request

Situation. A donor requests a monitoring visit to an education project in a district where three NGO vehicles were carjacked last month. National staff at the base ask why international staff have a protective vest and an evacuation option by air, while they have neither adequate insurance nor training. A young international coordinator volunteers for the visit "because he is not afraid".

Task. 1) Is the level of risk justified by the criticality of the activity? 2) What duty of care problems do you see? 3) What decision and what measures?

Answer. 1) A monitoring visit to an education project is not a life-saving activity: it does not justify a high risk. Alternatives should be sought: remote monitoring (calls, geotagged photos, local partner), verification by a better-accepted third party, postponement, or a meeting in a safer location. 2) Unequal treatment between national and international staff (insurance, training, equipment, relocation options); a decision left to individual volunteering instead of a risk assessment and a management decision. 3) Refuse the mission in this form and explain the alternative monitoring solution to the donor; launch a review of the measures for national staff (training, insurance, a relocation plan for those exposed because of their employment); restate that the risk threshold is set by management and not by volunteering.

Key takeaways

- Security risk management serves access to populations; it does not aim for zero risk.
- Duty of care: assess, inform, train, equip, respond and learn, equitably across all staff.
- Cycle: context, assessment, strategies, plans, implementation, monitoring and review.
- Acceptance first; protection as needed; deterrence as a last resort.
- Acceptable risk depends on programme criticality and is set by senior management, in writing.

Quiz

1. The core security strategy of humanitarian organisations is:
   A. Deterrence
   B. Acceptance
   C. Protection
   D. Total avoidance

2. Duty of care applies:
   A. To all staff, and to varying degrees to consultants, volunteers and visitors
   B. To international staff only
   C. Only to armed personnel
   D. Only in wartime

3. Who sets the acceptable risk threshold?
   A. The local authorities
   B. The most experienced staff member
   C. The donor
   D. The organisation's senior management, in writing

4. Armed guards around a warehouse fall under:
   A. Acceptance
   B. Unarmed protection
   C. Deterrence
   D. Avoidance

5. A staff member refuses a mission they judge too dangerous. They:
   A. Must be sanctioned
   B. Are exercising their right to withdraw, without sanction
   C. Must resign
   D. Must find a replacement

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