HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

Humanitarian Mini MBA: leading a humanitarian organisation

Course handout · Week 10 : Organisational risk and security management

A leadership programme of exactly 3 months (12 weeks, 144 hours): leadership, strategy, project cycle, MEAL, finance and donor budgets, compliance and fraud, resource mobilisation, supply chain, HR and safeguarding, risk and security, negotiation and advocacy, change and governance. Corrected numerical exercises, three demanding monthly exams with case studies, and a verifiable diploma from the Humanitarian Academy.

https://humanitairejobs.org/en/academy/mini-mba-humanitaire/semaine-10/

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

Week 10 : Organisational risk and security management

Objectives

- Set up organisation-wide risk management: register, risk appetite, residual risks, risk sharing with donors and partners.
- Lead security risk management: context analysis, threats, vulnerabilities, acceptance, protection and deterrence strategies.
- Prepare and lead critical incident management: crisis cell, communication, business continuity.

Organisational risk management

The **ISO 31000** standard defines risk as the effect of uncertainty on objectives. A humanitarian organisation faces risks of several kinds: **security**, **fiduciary** (fraud, corruption, diversion), **legal and compliance** (sanctions, labour law, data protection), **operational** (access, supply disruption), **reputational**, **ethical** (abuse, breach of principles) and **financial** (exchange rates, cash flow, donor dependence).

The **risk register** describes each risk (cause, event, consequence), its likelihood and impact (often on a scale of 1 to 5), the existing measures, the **residual risk**, the owner and the review date. The risk level is often calculated as likelihood × impact: a risk with likelihood 4 and impact 5 scores 20 out of 25, above an escalation threshold set, for example, at 15.

Risk appetite, approved by the board, states which risks the organisation accepts in order to fulfil its mission. A medical NGO may accept a high security risk to provide care in a conflict zone, but accept no risk at all of tolerating sexual exploitation. Without a formal risk appetite, every decision depends on the personality of the director in post.

> **Risk transfer** to local partners is a drift denounced by many studies: the international NGO stays sheltered while its partner carries the danger without means. **Risk sharing** means funding partners' security, sharing information and deciding together what is acceptable.

Security risk analysis

Security risk management follows a cycle: **context analysis** (actors, conflict dynamics, crime, perception of the organisation), **threat identification** (kidnapping, armed attack, road robbery, explosive devices, sexual violence, arbitrary detention, civil unrest, natural disasters, disease), **analysis of vulnerabilities** and capacities, then risk assessment and choice of measures.

A teaching formula sums up the logic: **risk = threat × vulnerability / capacities**. You almost never control the threat; you act on vulnerability (exposure, profile, predictable routines) and

on capacities (training, communications, procedures, network).

The **acceptable risk threshold** is decided by weighing residual risk against **programme criticality**: the more an activity saves lives, the higher the risk that can be accepted, with reinforced measures. The UN system's Programme Criticality framework and the approach of the Global Interagency Security Forum (GISF) formalise this reasoning.

Information sources must be cross-checked: network of local contacts, NGO security forums and security advisory organisations, UN agencies, local media, public conflict data (for example the Uppsala Conflict Data Program, UCDP). Sensitive information received from partners or third parties is not passed on without their consent.

Strategies: acceptance, protection, deterrence

The **security triangle** distinguishes three complementary strategies:

- **Acceptance**: reduce or remove the threat by obtaining the consent of actors (communities, authorities, armed groups) through quality, perceived impartiality, transparency and dialogue. It is the preferred strategy of NGOs, but it is built over time and can collapse quickly if an actor judges the organisation to be partial.
- **Protection**: reduce vulnerability through physical and procedural measures (walls, guards, suitable vehicles, movement procedures, hibernation, reduced visibility).
- **Deterrence**: pose a counter-threat (armed escorts, conditional withdrawal, political pressure). Armed escorts are in principle a last resort, governed by the IASC guidelines on the use of armed escorts, because they can compromise perceived neutrality and create new risks.

A country **security plan** includes: risk analysis, security levels and indicators for moving from one level to another, standard operating procedures (movements, communications, cash management, visitors), contingency plans (hibernation, relocation, evacuation) and a crisis organisation chart. It must be known, understood and tested through exercises, otherwise it is useless.

> Trigger indicators: decide in advance which events move you from one level to another (for example two armed incidents less than 20 km from the base in one week). Without indicators, the decision to relocate often comes too late.

Critical incident management

A **critical incident** (kidnapping, death, serious assault, attack on an office, disappearance) exceeds normal management capacity. It is managed by a **crisis management team** at headquarters or regional level, separate from the team on the ground, with roles defined in advance: crisis lead, family liaison, communication, security, legal and insurance, human resources, psychological support.

Principles for the first hours: **secure** the people still exposed, **verify** the facts, **activate** the crisis cell, **keep a log** of all decisions and information in chronological order, **control communication** (no public statements or social media posts by staff, a single spokesperson),

inform the family before any other audience, and **coordinate** with the authorities and other organisations.

In the event of a kidnapping, organisations rely on specialists and on their insurance; policies vary on paying ransoms, which several states prohibit or strongly discourage and which in some cases breaches sanctions regimes. The organisation's policy must be clear before the incident, not improvised during it.

After the incident: psychological support for the people affected and the team, a no-blame lessons-learned review, an update of the risk analysis and, where necessary, a review of the presence in the area.

Business continuity and reputation

Business continuity prepares the organisation to keep its essential functions running despite a disruption: loss of an office, communications or banking cut, epidemic, cyberattack, suspension of registration. The plan identifies **critical functions** (payroll, payments to beneficiaries, life-saving supplies, communication with donors), their maximum acceptable interruption time, and fallback solutions (off-site backups, alternative bank accounts, signature delegations, remote management).

Remote management (programmes run by national teams or partners when senior staff can no longer access the area) requires particular attention: real transfer of security resources, third-party monitoring systems, verification calls to beneficiaries, and vigilance not to transfer the risk without transferring the means.

Reputational risk often stems from other risks: an abuse scandal, a concealed fraud or a badly managed incident cost far more than their direct losses. The best protection is transparency: inform donors and, where appropriate, the public, factually and quickly, showing the measures taken.

Cybersecurity and data protection are now major risks: two-factor authentication, backups, updates, anti-phishing training, and encryption of sensitive beneficiary data.

Exercise: risk register and relocation decision

Part 1. Draw up a register of five risks for your organisation (at least one security, one fiduciary, one reputational, one data protection and one financial): cause-event-consequence description, likelihood and impact out of 5, score, existing measures, residual risk, owner. Indicate which ones exceed an escalation threshold of 15.

Part 2. Your Morongo base is at security level 3 out of 4. In ten days: two carjackings of NGO vehicles on the main road, leaflets hostile to foreign organisations, and the announcement of a military operation within 15 days. The base runs a nutrition programme treating 600 children with severe acute malnutrition. Analyse the situation (threats, vulnerabilities, criticality) and propose a reasoned decision: stay with measures, reduce staff, remote management or relocation. Specify the indicators that would trigger the next step and how to ensure continuity of care.

Answer key. Criticality is very high (life-saving treatment of children), which justifies accepting a higher risk, but not exposure without measures. A sound response reduces exposure (non-essential staff relocated, limited and unpredictable movements, reduced visibility), strengthens acceptance (dialogue with leaders about the leaflets), prepositions three months of nutrition products, gradually hands continuity of care over to health facilities and community health workers, and sets clear indicators for full relocation (fighting within a given distance, a direct threat against the organisation, inability to communicate).

Key takeaways

- Risk register: cause, event, consequence, likelihood × impact, residual risk, owner, review.
- Risk appetite approved by the board; share risks with partners, do not transfer them.
- Risk = threat × vulnerability / capacities; the acceptable threshold depends on programme criticality.
- Acceptance, protection, deterrence; armed escorts as a last resort.
- Critical incident: crisis cell, decision log, a single spokesperson, the family informed first.

Quiz

1. A fraud risk has likelihood 3 and impact 4; a kidnapping risk has likelihood 2 and impact 5. Risks scoring 12 or more are escalated. Which ones?
   A. None
   B. Fraud only (12); kidnapping is at 10
   C. Kidnapping only
   D. Both
2. Holding regular meetings with community leaders to explain targeting criteria is part of the strategy of:
   A. Deterrence
   B. Protection
   C. Acceptance
   D. Risk transfer
3. After a kidnapping, the first people to inform, before any public statement, are:
   A. Journalists
   B. The family of the kidnapped person, by the designated member of the crisis cell
   C. Donors
   D. The organisation's social media
4. Why set indicators in advance for moving from one security level to another?
   A. To satisfy donors
   B. So that the decision to reduce or relocate does not depend on the mood of the moment and is not taken too late
   C. To avoid training staff
   D. Because the law requires it
5. An international NGO hands over the activities in an area that has become too dangerous for its own staff to a local partner, with no additional security budget. This is:
   A. Good localisation practice
   B. A risk transfer, contrary to fair risk sharing
   C. A deterrence strategy
   D. A donor obligation

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