HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

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

Course handout · Week 3 : Assessing risks: threats, vulnerabilities, likelihood and impact

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-3/

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

Week 3 : Assessing risks: threats, vulnerabilities, likelihood and impact

Objectives

- Identify threats and assess the vulnerability of the organisation and of each staff profile to them.
- Score risks on a likelihood × impact matrix, calculate the residual risk after measures and compare it with the acceptable threshold.
- Write a clear, dated, reviewable risk assessment that leads to decisions.

Threat, vulnerability, risk

Three notions not to be confused:

- **Threat**: what can cause harm (carjacking, kidnapping, shelling, explosive device, riot, disease, road accident).
- **Vulnerability**: the degree to which the organisation or a person is exposed to that threat, depending on location, movements, profile, assets, procedures and acceptance.
- **Risk**: the combination of the likelihood that a threat materialises against us and the impact if it does.

The same threat does not create the same risk for everyone. **Example:** the threat of kidnapping for ransom weighs more heavily on profiles perceived as "profitable" (international staff of certain nationalities, senior national managers, people whose family is perceived as wealthy). Vulnerability also depends on procedures: predictable movements, always at the same times, increase everyone's vulnerability.

The likelihood × impact matrix

The most widespread method scores each risk on two scales from 1 to 5:

- **Likelihood**: 1 very unlikely, 2 unlikely, 3 possible, 4 likely, 5 very likely (over a defined period, for example 12 months).
- **Impact**: 1 negligible, 2 minor (limited material damage), 3 moderate (minor injuries, short interruption), 4 severe (serious injuries, loss of major assets, suspension), 5 critical (death, kidnapping, withdrawal from the country).

Score = likelihood × impact, from 1 to 25. Usual levels: 1 to 4 low, 5 to 9 medium, 10 to 16 high, 20 to 25 very high (thresholds vary between organisations and must be written down).

Threat	Likelihood	Impact	Score	Level
Carjacking on the northern route	4	4	16	High
Office burglary	3	2	6	Medium
Kidnapping of a staff member	2	5	10	High
Serious road accident	3	5	15	High

Note: road accidents often score as high as threats linked to violence, and they are easier to reduce.

Residual risk and the acceptable threshold

Inherent risk is the risk before measures; **residual risk** is what remains after the planned measures. The decision is taken on the residual risk, compared with the acceptable threshold set by senior management for the activity concerned.

Example. Carjacking on the northern route: inherent 4 × 4 = 16. Measures: two-vehicle movements, variable timings, no cash or valuables visible, communications with hourly check-in calls, daily update on road conditions from the NGO forum, a non-resistance rule. Estimated likelihood reduced to 2 (vulnerability falls), impact reduced to 3 (non-resistance, rapid assistance). Residual: 2 × 3 = 6, medium level.

If the acceptable threshold for distribution activities is "medium", the activity can continue with these measures. If the measures do not bring the risk below the threshold, the activity must be changed (modality, location, partner) or suspended.

> A measure that is written down but not applied reduces no risk. The assessment must state who applies what, and how it is checked.

The limits of scoring

The matrix is useful but misleading if taken as an exact measurement:

- Scores are **judgements**, not measurements. Two people may score differently; a reasoned consensus is sought, with national staff.
- **Rare, catastrophic events** (an attack on a hotel, a bombing of a base) have a low likelihood but an extreme impact: a score of 1 × 5 = 5 classifies them as "medium" even though they require specific plans.
- **Cumulative** risks: several medium risks combined can amount to an unacceptable situation.
- Risks change: an undated assessment, or one that is eight months old in an unstable context, is worthless.

Good practice: keep a particular eye on any threat with an impact of 5, whatever its likelihood, and prepare a contingency plan for each (kidnapping, armed attack, medical evacuation).

Profiles and inclusive security

People are not exposed in the same way depending on their **profile**: nationality, ethnic origin or clan, religion, gender, sexual orientation and gender identity, disability, age, appearance, language. The same place can be safe for one person and dangerous for another.

An **inclusive** approach to security (developed notably by GISF) consists of:

- taking profiles into account in the risk assessment, without forcing anyone to disclose personal information;
- allowing everyone to report concerns linked to their profile confidentially;
- adapting measures (accommodation, movements, postings), without automatically excluding people from certain positions;
- training managers on these issues.

Example. A national staff member from a minority ethnic group cannot cross certain checkpoints without risk. Rather than excluding him from the project, the team adapts the routes, assigns him to areas where his profile is not exposed, and arranges safe accommodation in case of tension.

Writing the assessment

A useful security risk assessment contains:

- the **area** and **period** covered, the date and the authors;
- a summary of the context (with reference to the analysis);
- the table of threats with likelihood, impact and inherent score;
- for each high or very high risk: measures, persons responsible, residual risk;
- the comparison with the acceptable threshold by type of activity;
- decisions and recommendations (continue, adapt, suspend);
- the date of the next review and the triggers for an early review.

It is **approved** by the country director (and by headquarters above a certain level of risk) and **explained** to the staff concerned. It also serves as the basis for the security budget and for staff informed consent.

Exercise: assess and decide

Situation. An NGO wants to open a base in a town 120 km from the regional capital. Threats identified: carjacking (likelihood 4, impact 4); armed attack on the base (likelihood 2, impact 5); kidnapping (likelihood 2, impact 5); road accident (likelihood 4, impact 4); serious illness without access to care (likelihood 3, impact 4). Acceptable threshold set by senior management for life-saving health activities: residual "high" at most (≤ 16), with a contingency plan for any threat with an impact of 5. Proposed measures: two-vehicle convoys and check-in calls (carjacking brought down to 2 × 3), road rules and trained drivers (accident brought down to 2 × 4), unarmed guards, wall and safe room (attack brought down to 1 × 5), medical evacuation through a contracted air service and medical kits (illness brought down to 2 × 3). No specific measure for kidnapping.

Task. 1) Inherent and residual scores. 2) Is the opening acceptable? 3) What is missing?

Answer. 1) Inherent: carjacking 16, attack 10, kidnapping 10, accident 16, illness 12. Residual: carjacking 6, attack 5, kidnapping 10 (unchanged), accident 8, illness 6. 2) All residual scores are ≤ 16, so within the threshold, but two threats with an impact of 5 (attack, kidnapping) require a contingency plan. 3) Measures and a plan for kidnapping are missing: analysis of exposed profiles, low-profile movements, varied timings, rules on visitors, preparation of a crisis management team and a kidnap management policy; and a contingency plan in case of attack (safe room, back-up communications, relocation procedure). The opening can be decided once these plans are in place and approved by senior management.

Key takeaways

- Risk = likelihood × impact of a threat, depending on the vulnerability of the organisation and of individuals.
- Decide on residual risk, compared with the acceptable threshold for the activity.
- A measure that is not applied reduces nothing: named responsibilities and verification are mandatory.
- Any threat with an impact of 5 requires a contingency plan, whatever its likelihood.
- Inclusive security: take profiles into account without excluding people or forcing disclosure.

Quiz

1. Likelihood 3, impact 5. The score is:
   A. 8
   B. 35
   C. 2
   D. 15

2. After measures, a risk goes from 4 × 4 to 2 × 3. The residual risk is:
   A. 16
   B. 10
   C. 6
   D. 8

3. A threat with a likelihood of 1 and an impact of 5 (score 5):
   A. Can be ignored
   B. Requires a specific contingency plan
   C. Is automatically acceptable
   D. Must be scored 25

4. The decision to continue an activity is taken on:
   A. The residual risk compared with the acceptable threshold
   B. The inherent risk
   C. The donor's opinion
   D. Last year's number of incidents

5. In an inclusive security approach, you:
   A. Automatically exclude certain profiles
   B. Require everyone to declare their sexual orientation
   C. Ignore profiles
   D. Allow confidential reporting and adapt measures

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