HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

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

Complete manual

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/

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

Contents

1. Week 1 : Duty of care and security risk management: the framework
2. Week 2 : Analysing the context: actors, dynamics and trends in violence
3. Week 3 : Assessing risks: threats, vulnerabilities, likelihood and impact
4. Week 4 : Security plans, procedures, movements and communications
5. Week 5 : Building acceptance and negotiating access
6. Week 6 : Incidents: report, analyse, learn
7. Week 7 : Managing a crisis: crisis management team, hibernation, relocation, evacuation, kidnapping
8. Week 8 : Health, psychosocial wellbeing, internal safeguarding and insurance
9. Week 9 : Digital security and information protection
10. Week 10 : Managing all the organisation's risks: register, appetite, compliance and reputation
11. Week 11 : Sharing risk with partners and funding security
12. Week 12 : Governance, security culture, business continuity and final project

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

Week 2 : Analysing the context: actors, dynamics and trends in violence

Objectives

- Conduct a structured context analysis (political, economic, social, security) that is useful for decision-making.
- Map actors according to their influence, their interests and their attitude towards the organisation.
- Read incident data (frequencies, rates, trends) without misinterpretation, and produce early warning indicators.

Why analyse the context

All security decisions rest on an understanding of the context. A weak analysis produces two symmetrical errors: **underestimating** a threat (and exposing staff) or **overestimating** it (and abandoning populations who could have been helped).

A good analysis answers a few questions: who controls the territory and the roads? What are the actors' interests, and how does humanitarian action affect them? What types of violence exist, against whom, where, when and why? What is changing?

Sources: national staff (the first source, often the most nuanced), communities, authorities, other organisations, NGO security coordination forums, the United Nations (UNDSS), local media, social media (with caution), public conflict databases. All information is **cross-checked** and rated according to the reliability of the source and the credibility of the information.

Analytical frameworks

Two simple frameworks structure the analysis:

- **Adapted PESTEL**: political, economic, social, technological, environmental, legal, to which security is added (armed groups, crime, security forces).
- **Historical analysis**: a timeline of major events over recent years, to identify cycles (fighting seasons, election periods, harvests, transhumance).

The analysis leads to **scenarios**: the most likely, the most dangerous, and possibly an improvement scenario, each with observable **indicators** that signal it is approaching.

Example of indicators. Scenario "resumption of fighting around the town": families moving south, closure of weekly markets, sudden rise in fuel prices, departure of foreign traders, reported troop movements, hostile rhetoric on local radio stations. Three out of six indicators observed trigger a crisis meeting and a review of the security level.

Mapping actors

Actor mapping lists those who can influence security and access: national and local authorities, armed forces and police, non-state armed groups, traditional and religious leaders, militias, criminal networks, traders, media, host and displaced communities, other organisations.

For each: **influence** (low to high), **attitude** towards the organisation (hostile, neutral, favourable), **interests** and current **relationship**.

Actor	Influence	Attitude	Action
Leader of the main militia	High	Neutral, suspicious	Regular dialogue through an accepted intermediary; explain the principles and the targeting criteria
Prefect	High	Favourable	Regular information, compliance with administrative procedures
Unemployed young people in the town	Medium	Hostile (recruitment seen as unfair)	Transparent recruitment, complaints mechanism, fair daily-labour jobs

> A hostile actor with high influence is a priority for the analysis and for the acceptance strategy, not just a threat to be avoided.

Reading incident data

Incident data help to objectify the threat, provided they are read correctly:

- **Raw frequency**: number of incidents per period.
- **Rate**: incidents relative to exposure (number of staff, trips, person-days). Without a denominator, an increase may simply reflect an increase in activity.
- **Reporting bias**: an increase may come from better reporting, not from a deterioration.
- **Typology**: the same total can hide a fall in thefts and a rise in kidnappings, which are far more serious.

Example. Year 1: 24 incidents for 300 staff. Year 2: 36 incidents for 600 staff. Rates: 8 versus 6 incidents per 100 staff per year. Despite a raw increase of 50%, the rate has fallen by 25%. But if serious incidents (violence against people) go from 3 to 9, their rate goes from 1 to 1.5 per 100 staff: severity is increasing. The reading combines rate and severity.

Understanding violence against aid workers

Attacks on aid workers follow several logics, which must be distinguished because they call for different responses:

- **Criminal**: financial gain (thefts, robberies, kidnappings for ransom). Protection measures and discretion about valuables are effective.

- **Political or military**: the organisation is perceived as an ally of one side, or its action disrupts a strategy. Acceptance, perceived neutrality and communication are central.
- **Linked to the work itself**: targeting disputes, contested recruitment, dismissals, unaddressed complaints. Programme quality and accountability are security measures.
- **Incidental**: being in the wrong place at the wrong time (crossfire, shelling, mines). Analysis of areas and timings, movement procedures.

Many serious incidents affecting NGOs are linked to **internal or neighbourhood tensions** (dismissed staff member, rejected supplier, excluded beneficiary): security analysis must also look at the organisation itself.

Producing a useful analysis

A useful analysis fits on **two pages**, is updated regularly (monthly in an unstable context, after any major event), and ends with concrete implications:

- areas and roads that are accessible, accessible under conditions, or off-limits;
- travel times and modes of transport;
- actors to meet and key messages;
- indicators to monitor and review thresholds;
- consequences for programmes (timetable, modalities, remote management).

It is shared with the people who need it, while respecting **confidentiality**: an analysis that names armed actors or informants can put people in danger if it circulates. Nor should it use confidential information from other organisations without their explicit agreement.

Exercise: a changing town

Situation. An NGO has been working for 3 years in a garrison town. Data: year 1, 18 incidents for 150 staff (including 2 against people); year 2, 27 incidents for 300 staff (including 6 against people). Over the past month: a local candidate who was not recruited has publicly threatened the organisation; two weekly markets have closed; rents are falling as well-off families leave; a local radio station accuses "the NGOs" of helping the rebels; the NGO security forum reports troop movements.

Task. 1) Calculate and interpret the incident rates. 2) Classify the signals by logic of violence. 3) Propose three practical implications.

Answer. 1) Overall rate: 12 then 9 incidents per 100 staff (a fall of 25%). Rate of incidents against people: 1.33 then 2 per 100 staff (a rise of 50%). The situation is getting worse in severity despite the fall in the overall rate. 2) Threat from the unsuccessful candidate: work-related logic; radio accusations: political logic (perception of partiality); closed markets, departures, troop movements: indicators of a scenario of renewed fighting (incidental and political risk). 3) Address the recruitment complaint (formal mechanism, transparency, security of HR staff); launch an acceptance effort (meetings with authorities and leaders, a radio programme on principles and aid criteria); review the scenario and the security level, and prepare relocation and remote management if the military indicators are confirmed.

Key takeaways

- A weak analysis underestimates or overestimates; cross-check and rate source reliability and credibility.
- Scenarios with observable indicators and thresholds that trigger a review.
- Map actors' influence, attitude and interests; prioritise influential hostile actors.
- Always use a denominator: incident rates per exposure, read together with severity.
- Many serious incidents have a work-related origin: programme quality is a security measure.

Quiz

1. 30 incidents for 500 staff. The rate per 100 staff is:
   A. 30
   B. 16.7
   C. 6
   D. 0.6

2. Incidents go from 20 to 30 while staff numbers go from 200 to 400. The rate:
   A. Rises by 50%
   B. Falls by 25%
   C. Remains stable
   D. Doubles

3. A badly handled dismissal followed by threats is mainly a form of violence:
   A. Linked to the organisation's work
   B. Incidental
   C. Criminal
   D. Military

4. A security analysis that names informants must:
   A. Be published for transparency
   B. Be shared with all partners
   C. Be sent to the media
   D. Circulate on a strictly restricted basis so as not to put them in danger

5. A hostile and highly influential actor must be:
   A. Ignored
   B. Reported to the press
   C. A priority for the analysis and the acceptance strategy
   D. Bypassed without ever being contacted

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

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

Week 4 : Security plans, procedures, movements and communications

Objectives

- Write a country or area security plan, with security levels and associated measures.
- Design realistic standard operating procedures, in particular for movements and sites.
- Set up a communications and movement tracking system that works when everything else fails.

The security plan

The **security plan** translates the risk assessment into rules and responsibilities. It is short, practical, known to everyone and regularly reviewed. Typical contents:

- summary of the context and the main threats;
- strategy (mix of acceptance, protection, deterrence);
- security levels and associated measures;
- standard operating procedures (movements, sites, communications, visitors, cash, incidents);
- contingency plans (medical evacuation, hibernation, relocation, evacuation, kidnapping, attack);
- security organisation chart and emergency contacts;
- annexes: maps, staff lists, inventory of communications equipment.

Every new arrival receives a **security briefing** on arrival and signs to confirm they have read the plan. An 80-page plan that nobody has read protects nobody.

Security levels

Most organisations use 4 or 5 **security levels** per area, each associated with automatic measures, which speeds up decisions in times of tension:

Level	Situation	Typical measures
1. Normal	Low, stable risks	Standard procedures
2. Vigilance	Tensions, isolated incidents	Movements restricted to certain hours, reinforced check-in calls, review of plans
3. Restriction	Rising violence, possible targeted threats	Essential movements only, with authorisation; reduction of non-essential staff; adapted activities
4. Hibernation or relocation	Widespread or targeted violence	Staff gathered in a safe location, or departure of the most exposed staff; activities suspended or managed remotely
5. Evacuation and suspension	Unacceptable risk	Departure from the area or the country according to the plan; contact maintained with staff who remain

Moving from one level to another is decided by the country director, on the basis of **indicators** defined in advance (see week 2), and communicated immediately to everyone.

Movement procedures

Movements are when staff are most exposed. Typical procedure:

- Prior **authorisation** according to the security level, based on a movement plan: route, timings, passengers, vehicles, contacts.
- **Route check** on the morning of travel: security forum, authorities, transporters, local staff.
- **Vehicle** checked and equipped: fuel, spare wheel, first aid kit, communications.
- **Check-in calls** at set intervals and at each key point; a clear procedure if a call is missed.
- **Internal curfew**: arrival before a set time, with a margin.
- **Behaviour** at checkpoints and in the event of a carjacking (no resistance, no photos, calm, cooperation).

Departure calculation. A 180 km journey at a realistic average speed of 40 km/h: 4 hours 30 minutes. Internal curfew 17:00, one-hour margin: planned arrival no later than 16:00. Departure no later than 11:30. With a check-in call every hour and on arrival: 5 calls. If a call is missed, the base tries to make contact again for 15 minutes, then triggers the missing vehicle procedure.

Site security

Offices, residences, warehouses and distribution sites are assessed and given appropriate measures:

- **Site selection**: neighbourhood, surroundings (avoid proximity to potential targets: military buildings, sensitive ministries), two access routes, distance from flood-risk areas.
- **Perimeter**: wall or fence, gate, lighting, trained unarmed guards, visitor control.
- **Building**: solid doors and windows, safe room or shelter depending on the threats (room reinforced against intrusion, shelter against indirect fire).

- **Fire and electrical safety**: extinguishers, detectors, emergency exits.
- **Stocks**: water, food, fuel and medicines for hibernation (often 7 to 14 days).

Stock calculation. 12 people, 10-day hibernation: water at 4 litres per person per day for drinking and minimal use = 480 litres; with a 20% margin, about 580 litres. Food: 12 × 10 = 120 daily rations. Fuel for a generator at 2 litres per hour, 8 hours a day: 160 litres.

Communications

The communications system must work **when the mobile network is down**, which often happens just when it is most needed. Principle of redundancy: at least two independent means.

- **Mobile phone**: convenient, but fragile and open to surveillance.
- **HF radio**: long range, independent of networks, but requires trained operators and licences.
- **VHF radio**: short range, ideal in town and in convoys, with repeaters.
- **Satellite phone** and satellite data terminals: independent, but expensive and sometimes regulated or viewed with suspicion by the authorities.
- GPS **tracking devices** with a panic button.

Rules: call signs, plain language but no sensitive information (no names, cash amounts or detailed routes over the radio), call tree (each manager calls a defined number of people), regular tests, chargers and back-up batteries. Communications are also an acceptance issue: using a radio or satellite phone where the authorities forbid it can lead to suspicions of spying.

Procedures that are actually applied

Procedures often fail for simple reasons: too many of them, poorly known, impossible to apply, or bypassed out of habit. Good practice:

- Write **few** procedures, short ones, adapted to the real context, with the staff who will apply them.
- **Explain** them (the why) rather than just imposing them.
- **Practise** them: simulations of a missing vehicle, hibernation, medical evacuation, at least twice a year.
- **Check** them: spot checks of logbooks, check-in calls, visitor registers.
- Treat non-compliance as a **management** issue: a manager who bypasses procedures sets an example for the whole team.

> Complacency is a risk in its own right: after months without incident, procedures slacken precisely when the context may tip over.

Exercise: planning a field mission

Situation. A team of 4 people must travel from the base to a site 210 km away for a distribution. Realistic average speed: 35 km/h. Internal curfew: 17:30, with a one-hour margin. The distribution lasts 3 hours. The site has no mobile network over the last 80 kilometres. The security level of the area is "vigilance". The driver suggests leaving at 09:00 "as usual".

Task. 1) Can the mission be done as a return trip in one day? 2) If not, how should it be organised? 3) What means of communication and what check-in calls?

Answer. 1) Journey: 210 / 35 = 6 hours. Return trip 12 hours + 3 hours of distribution = 15 hours; arrival no later than 16:30: departure at 01:30, which is impossible (no night-time driving). The mission cannot be done in a day. 2) Overnight stay on site or in a safe stopover town, in accommodation assessed in advance; or split it up: day 1 travel (departure at 09:00, arrival around 15:00), day 2 distribution and partial return, or distribution by a local partner with monitoring. Vary the usual departure time, which makes movements predictable. 3) Mobile phone where there is a network, satellite phone or HF radio for the 80 km without network, tracking device; check-in call every hour and at each key point (departure, entry into the area without network, arrival, start and end of distribution); missing vehicle procedure known to the base.

Key takeaways

- A short security plan, known to all, signed on arrival, regularly reviewed.
- Security levels with automatic measures and escalation indicators defined in advance.
- Movements: authorisation, route check, check-in calls, curfew with a margin, non-resistance.
- Redundant, tested communications, with no sensitive information in plain language.
- Few procedures, explained, practised and checked; complacency is a risk.

Quiz

1. A 160 km journey at 40 km/h, arrival no later than 16:00. Latest departure:
   A. 12:00
   B. 10:00
   C. 14:00
   D. 11:00

2. 10 people, 7 days of hibernation, 4 litres of water per person per day. Minimum water:
   A. 70 litres
   B. 400 litres
   C. 40 litres
   D. 280 litres

3. Why require two independent means of communication?
   A. To reduce costs
   B. Because donors require it
   C. Because the mobile network often fails at the critical moment
   D. To communicate with the press

4. On the radio, you avoid mentioning:
   A. Call signs
   B. Names, cash amounts and detailed routes
   C. The time
   D. The security level

5. After six months without incident, the team relaxes check-in calls. This is:
   A. Complacency, a risk to be corrected by management
   B. Normal and risk-free
   C. A good adaptation
   D. A decision for the driver

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

Week 5 : Building acceptance and negotiating access

Objectives

- Build an acceptance strategy grounded in principles, programme quality and dialogue with all actors.
- Measure acceptance with concrete indicators rather than assuming it.
- Prepare and conduct a humanitarian access negotiation with an armed actor, setting your red lines.

Acceptance cannot be taken for granted

Acceptance is the active or passive consent of the actors who can harm the organisation. It cannot be decreed: it is built and maintained, and it can be lost in a single day.

It rests on several pillars:

- **Principles**: humanity, neutrality, impartiality, independence, understood and perceived as real.
- The **quality and relevance** of programmes: aid that is useful, fair and well targeted.
- **Accountability**: communities know what they can expect and can complain.
- Staff **behaviour**: respect, discretion, no arrogance, no exploitation or abuse.
- **Dialogue** with all actors who have influence, including non-state armed groups.
- **Consistency**: the same criteria everywhere, the same message to everyone.

Acceptance is often **local and personal**: it depends on a team, on a respected manager. It is not automatically transferred from one area to another, or from one person to another.

What destroys acceptance

Losses of acceptance often come from the organisation itself:

- Targeting perceived as unfair or captured by an elite or a group.
- Recruitment perceived as favouring a clan or excluding the local population.
- Broken promises, programmes stopped without explanation.
- Visible association with a party to the conflict (military escorts, armed forces logos, presence at publicised military meetings).
- Personal behaviour: dangerous driving, conspicuous alcohol consumption in a conservative context, relationships seen as inappropriate.
- Careless public communication: a headquarters press release or a social media post read locally as taking sides.

> One tweet from headquarters can undo months of acceptance work in the field: external communication is part of risk management.

Measuring acceptance

Acceptance is too often assumed ("people like us"). It can be **measured** with indicators:

- Do communities and leaders know the organisation, its activities and its principles? (perception surveys, interviews)
- Does the organisation receive spontaneous **warnings** ("don't go that way tomorrow")?
- Are its access requests granted, and how quickly?
- Do the complaints received concern the quality of the aid or the presence of the organisation itself?
- Do incidents target it more or less than other comparable organisations?

Example. Perception survey of 300 people in two districts: district A, 78% know the organisation and 70% consider the aid "fair"; district B, 41% know it and 35% consider the aid "fair". Acceptance is clearly weaker in B, where the team nonetheless felt "well accepted". Actions: community meetings, dissemination of targeting criteria, review of lists with committees, more balanced local recruitment.

Negotiating access: preparation

Humanitarian negotiation aims to obtain access to populations, the security of teams and respect for principles, in a dialogue that is often asymmetrical. Structured methods (for example those of the Centre of Competence on Humanitarian Negotiation, CCHN) stress preparation:

- **Analysis of the counterpart**: interests, motivations, norms, constraints, network, whom they themselves have to convince.
- **Analysis of your own mandate**: what you can offer, what you cannot.
- **Red lines** set and approved in advance by line management: no payments, no diversion of aid, no imposed beneficiary list, no escort by the armed group if it compromises neutrality.
- **Negotiation space**: the points open to exchange (timetable, modalities, communication, choice of sites).
- **Team**: who negotiates (an accepted person, language, profile), who supports, who decides.
- **Plan B**: what do you do if it fails? (best alternative to a negotiated agreement)

Negotiating access: conduct and follow-up

Principles of conduct:

- Start by building the **relationship** and trust; listen before asking.
- Talk about the **needs of the populations** that the counterpart claims to defend: many armed actors want to be seen as protecting "their" population.

- Explain the principles in concrete terms: impartiality = aid according to need, for everyone; neutrality = not taking sides, including against them.
- Never promise what you cannot deliver; never give in on a red line under pressure: ask for time and refer upwards.
- Keep a **record** of what is agreed, and inform the other actors concerned if necessary, without putting anyone in danger.

Follow-up. An access agreement is tested in practice: do the teams actually get through? Are commitments kept on both sides? Any violation (taxation, diversion, threats) is analysed and met with a proportionate response: reminder, partial suspension, total suspension, coordination with other organisations to prevent a group from playing the NGOs off against one another.

Coordination and common positions

Negotiating alone exposes the organisation to demands it cannot refuse without risk, or that another organisation will accept. **Coordination** strengthens everyone's position:

- **Common operating rules** (ground rules) between organisations in an area: no payments at checkpoints, no armed escorts except in exceptional cases, collective refusal of imposed lists.
- **Access working groups** led by OCHA, which monitor access constraints and carry joint advocacy.
- **NGO security forums** that share information and analysis.

Limits: coordination must not cost each organisation its **independence**, nor associate it with political positions. Some organisations, such as the ICRC, conduct their own confidential negotiations. Coordination is about principles and practices, not blind alignment.

Exercise: a checkpoint that "taxes"

Situation. An armed group controls the road to 3 displacement camps (25,000 people). For the past two weeks, it has been demanding USD 50 per aid truck and asking for 10% of the food to be "handed over to the fighters who protect the camps". Two NGOs have started paying "so as not to abandon people". Your organisation distributes food and runs a health centre. A recent perception survey shows that 74% of camp residents know you and consider your aid fair.

Task. 1) What are your red lines? 2) What levers and what interests of the group can you use? 3) What is your plan if the negotiation fails?

Answer. 1) No payment or share of the aid to a party to the conflict (a violation of principles, of donor rules and often of counter-terrorism laws); no distribution under the group's control; beneficiary list drawn up by the organisation according to need. 2) Levers: strong acceptance in the camps (the group wants to be seen as the protector of the displaced); the importance of the health centre, including for the fighters' families (impartial care for all); a common position with the other organisations through the access working group; the intervention of religious or traditional leaders respected by the group. 3) Coordinate with OCHA and the NGOs so that payments stop collectively; if access remains conditional, temporarily suspend food convoys while explaining why to the communities and to the group; consider alternative modalities (cash transfers if markets allow, local purchases in the camps); keep the health centre running if its access does not depend on the convoys; document and inform donors.

Key takeaways

- Acceptance is built, maintained and measured, and can be lost in a day.
- Targeting, recruitment, behaviour and public communication: the main causes of lost acceptance.
- Negotiating: analyse the counterpart, set red lines, know your negotiation space and your plan B.
- No payment or share of the aid to a party to the conflict: a common red line.
- Common rules between organisations strengthen each one, without sacrificing independence.

Quiz

1. Which sign indicates genuine acceptance?
   A. Staff feel good
   B. The community gives spontaneous warnings about dangers
   C. The donor is satisfied
   D. The offices are well protected

2. A negotiation red line must be:
   A. Set and approved in advance by line management
   B. Improvised during the meeting
   C. Negotiable if the counterpart insists
   D. Secret even from the team

3. An armed group demands 5% of the aid. The response consistent with principles:
   A. Accept in order to keep access
   B. Pay in cash rather than in food
   C. Accept in secret
   D. Refuse, seek a common position and other levers, suspend if necessary

4. Why coordinate common rules between organisations?
   A. To share budgets
   B. To remove each one's independence
   C. To prevent an actor from playing organisations off against one another
   D. To avoid talking to communities

5. In a survey, 40% of residents know the organisation in a district where the team believes it is well accepted. Conclusion:
   A. The survey is wrong
   B. Acceptance is probably overestimated; strengthen information and dialogue
   C. The district must be left
   D. Nothing to do

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

Week 6 : Incidents: report, analyse, learn

Objectives

- Set up an incident and near-miss reporting system that encourages information to flow upwards.
- Analyse an incident with a structured method (timeline, causes, contributing factors) without a blame culture.
- Use incident data to adjust measures and report to senior management and donors.

Why report

A **security incident** is any event that caused or could have caused harm to staff, assets, reputation or programmes. A **near miss** is an event that could have caused harm but did not: gunfire heard near a convoy, a fake checkpoint narrowly avoided, a verbal threat.

Reporting serves to:

- **provide assistance** immediately to the people affected;
- **alert** other teams and organisations;
- **understand** trends and adapt measures;
- **account** to senior management, the board, donors and insurers;
- **demonstrate** that the organisation is exercising its duty of care.

The incident pyramid (observed in many sectors) shows that before a serious incident there are generally many near misses and minor incidents. Not reporting them means depriving yourself of early warnings.

The reporting system

An effective system has three levels:

- **Immediate alert** (within the hour): a call or message to the designated person, with the essential information: who, what, where, when, condition of the people involved, need for help.
- **Incident report** (within 24 to 48 hours): a standard form with timeline, consequences, actions taken.
- **Analysis** (within 1 to 2 weeks for significant incidents): causes, lessons, recommendations.

To encourage reporting:

- a simple form, available offline and in staff languages;
- **no sanction** for reporting a good-faith error (a "just" culture, which distinguishes honest error from gross negligence or deliberate violation);
- a **confidential** channel for sensitive incidents (sexual violence, harassment, incidents involving a colleague);

- **feedback**: teams see what changes as a result of their reports.

> If a team never reports anything, it is almost never because nothing happens. It is a warning sign about the security culture.

Classifying incidents

A common **typology** makes data comparable: violence against people (murder, injury, kidnapping, sexual assault, arbitrary detention), theft and robbery, intrusion, threat, conflict-related incident (gunfire, shelling, explosive devices), road accident, health incident, digital security incident, civil unrest.

Each incident is also given a **severity level**, for example from 1 (minor, no injury or significant loss) to 4 (critical: death, kidnapping, serious injury, withdrawal from an area).

Example of a quarterly table. 42 incidents reported: 15 minor thefts, 9 threats, 6 road accidents (2 of them serious), 5 carjackings, 4 conflict-related near misses, 2 short arbitrary detentions, 1 physical assault. There are 8 incidents of severity 3 and 4, i.e. 19%. All 5 carjackings took place on the same route, between 15:00 and 17:00: the trend can be acted on (change of timings, review of authorisations on that route).

Analysing an incident

The analysis of a significant incident seeks to understand, not to punish. A four-step method:

- A precise **timeline**, reconstructed from several sources (people involved, witnesses, communications, GPS).
- **Facts and consequences**: damage, reactions, assistance provided.
- **Causes and contributing factors**: context (threat), vulnerabilities (procedures, behaviour, equipment), decisions taken and the reasons for them, what worked well.
- **Recommendations**: concrete measures, persons responsible, deadlines, and verification of their implementation.

Useful questions: was the threat known? Were the procedures appropriate? Were they known and applied? If not, why not (impossible, unknown, bypassed)? Was the response to the incident fast and appropriate? What should we have seen coming?

The people affected must be **protected** during the analysis: psychological support, respect for their pace, confidentiality, and no repeated questioning that re-traumatises them.

Using the data

Incident data feed into:

- the **context analysis** and the risk assessment (frequencies, locations, timings, perpetrators, modus operandi);
- **decisions** on measures (what works, what does not);
- **reports** to senior management (quarterly dashboard) and to the board;

- **sharing** with security forums and sector databases, in anonymised form and with the organisation's agreement.

Useful indicators. Number of incidents per 100 staff; share of serious incidents; average reporting time; share of recommendations implemented on time. **Example:** 24 recommendations from the year's analyses; 15 implemented on time, 5 late, 4 not started. On-time implementation rate: 62.5%. The 4 not started are examined as a priority by senior management: a recommendation that is not applied leaves the risk intact.

Reporting and communicating

After a serious incident, several audiences expect information, with different needs:

- The **family** of those affected: fast, humane information, from a designated person, before any public communication.
- **Staff**: factual information, measures taken, support available, to avoid rumours.
- **Donors**: depending on the contracts, rapid notification of serious incidents and their consequences for programmes.
- **Insurers**: notification within the deadlines for damage and medical costs.
- **Other organisations**: alert through the security forum.
- **Media**: only through the designated spokesperson; in the case of a kidnapping, public communication can put the victim in danger and is decided by the crisis management team.

Clumsy communication can make an incident worse: publishing a victim's name before the family has been told, publicly accusing an armed actor, or revealing information that compromises a negotiation.

Exercise: analysing a carjacking

Situation. One of the organisation's vehicles was carjacked at 16:40 on the southern route, 25 km from the base; the driver and two staff members were not injured, but the vehicle, two laptops and USD 4,000 in cash per diems were taken. Facts: the movement authorisation provided for arrival before 16:00; the distribution had been delayed; the 16:00 check-in call was not made (no network); the base manager did not trigger the missing vehicle procedure until 17:30. In the previous quarter, 3 near misses had been reported on the same route in the late afternoon, without any change to procedures. The cash per diems were being carried "to keep things simple".

Task. 1) Contributing factors. 2) What worked well. 3) Recommendations.

Answer. 1) Late departure without reassessment (curfew procedure not applied in the face of the delay); an area without network coverage and no alternative means of communication; a 90-minute delay before the missing vehicle procedure was triggered; previous near misses not acted upon; visible and unnecessary transport of cash. 2) Non-resistance by staff, with no injuries; immediate reporting after the incident. 3) A clear rule: in the event of a delay, stay on site in a safe place assessed in advance rather than driving on this route in the late afternoon; satellite phone or tracking device for areas without network coverage; missing vehicle procedure triggered no later than 15 minutes after a missed call; systematic analysis of near misses; payment of per diems by mobile money or bank transfer, and a ceiling on cash carried; psychological support for the three staff members; persons responsible and deadlines for each recommendation, monitored by the country director.

Key takeaways

- Report incidents and near misses: the base of the pyramid prevents the top.
- Three levels: immediate alert, report within 48 hours, analysis of significant incidents.
- Just culture: no sanction for an honest error that is reported; confidential channels.
- Analyse to understand: timeline, causes, contributing factors, recommendations followed up.
- After a serious incident: the family first, a single spokesperson, absolute caution in the event of a kidnapping.

Quiz

1. Gunfire heard near a convoy, with no injuries or damage, is:
   A. Nothing to report
   B. A serious incident
   C. A near miss to be reported
   D. A health incident
2. 48 incidents, 12 of them of severity 3 or 4. The share of serious incidents is:
   A. 12%
   B. 25%
   C. 36%
   D. 4%
3. 30 recommendations, 21 implemented on time. Rate:
   A. 70%
   B. 30%
   C. 21%
   D. 63%
4. In a just culture, a staff member who reports an honest error:
   A. Is sanctioned as an example
   B. Is transferred
   C. Must pay for the damage
   D. Is not sanctioned, and the error is used for learning
5. After a staff member is kidnapped, who decides on public communication?
   A. The headquarters communications department alone
   B. Each colleague on social media
   C. The crisis management team
   D. The local media

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

Week 7 : Managing a crisis: crisis management team, hibernation, relocation, evacuation, kidnapping

Objectives

- Organise a crisis management team and its first hours: roles, information, decisions, log.
- Plan and decide on hibernation, relocation or evacuation, including for national staff.
- Know the principles of managing a kidnapping or detention and the role of each person.

What is a crisis?

A **crisis** is a situation that seriously threatens people, the organisation's ability to function or its reputation, and that goes beyond ordinary procedures: kidnapping, violent death, attack on a base, evacuation from a country, a disaster affecting staff, a serious scandal.

Crisis management relies on a structure prepared in advance:

- **Crisis management team** (at headquarters or regional level): decides the strategy, mobilises resources, manages relations with families, authorities, donors and the media.
- **Incident management team** (at country level): manages the situation on the ground and implements decisions.

This separation allows the field to concentrate on action while the crisis management team manages the environment and strategic decisions. Both must have written terms of reference, designated members and alternates, and have carried out at least one simulation exercise.

The first hours

The first hours often determine the outcome of a crisis. Typical action list:

- **Activate** the team according to the agreed criteria; appoint a lead and a secretary who keeps the **crisis log** (time, information, source, decision, person responsible).
- **Establish the facts**: distinguish what is confirmed, probable, rumour.
- **Protect people**: move the rest of the staff to safety, medical assistance, regrouping.
- **Inform** families (through a designated person), staff and senior management; control external communication (no public comment without a decision by the crisis management team).
- **Take** urgent **decisions**: security level, suspension of activities, movements.
- **Plan** the next hours and the handovers: a crisis can last for weeks, and fatigue is a risk.

> The crisis log is not a formality: it keeps a record of decisions, protects the organisation legally and avoids repeating the same discussions at every handover.

Hibernation, relocation, evacuation

Three options when the situation deteriorates, described in the security plan:

- **Hibernation**: staying in place, gathered in a safe location, until the immediate danger passes (fighting in the town, riots). It requires stocks (water, food, fuel, medicines), communications and a decision on the maximum duration.
- **Relocation**: moving some of the staff to a safer area within the same country (capital, another region), generally the most exposed or non-essential staff.
- **Evacuation**: getting staff out of the country. For international staff, this often means returning to their home country; for national staff, evacuation out of the country is legally and practically complex, and rarely possible.

The **point of no return**: beyond a certain moment (airport closed, roads cut), evacuation is no longer possible. You must therefore decide **early**, on the basis of indicators, rather than waiting for certainty.

Evacuation calculation. 46 people to relocate by a 12-seat aircraft; 2 seats reserved for airline staff and communications equipment: 10 usable seats per rotation. 5 rotations are needed. If each rotation takes 3 hours and the airstrip closes at nightfall, only 3 rotations can be made per day: 2 days at least. The priority list (most exposed people, sick people, non-essential staff) is drawn up in advance.

National staff in crises

National staff are often the most exposed and the least protected during crises. Good practice:

- Discuss in advance with each staff member their own risks (profile, place of origin, family) and the realistic options.
- Provide **internal relocation** options for those who are threatened because of their employment.
- Guarantee **continuity of salaries** in the event of suspension (salary advances before an evacuation, remote payment methods).
- Maintain **contact** and support after international staff have left.
- Do not transfer responsibility for programmes to national staff or partners without resources or agreement, thereby exposing those who remain.

Example. Before an evacuation, an organisation pays a three-month salary advance to its 60 national staff, sets up a daily call tree, and agrees a simple protocol with them: no activity is maintained without an assessment and the agreement of each person, and no staff member keeps organisational assets that would put them in danger.

Kidnapping and detention

Kidnapping is one of the most serious and longest-lasting crises. Generally accepted principles (to be adapted to each organisation's policy and the applicable law):

- **Prevention**: analysis of exposed profiles, low profile, varied routes and timings, control of published information (including staff social media).
- **Preparation**: a written policy (including the organisation's position on ransoms, which varies between organisations and laws), confidential "proof of life" forms completed in advance by exposed staff (questions to which only the person knows the answer), specialist insurance where appropriate, specialist consultants identified.
- **Management**: a dedicated crisis management team, strictly controlled communication, coordination with the family and, depending on the case, with the authorities and governments concerned, support from specialists.
- **Afterwards**: long-term medical and psychological support for the released person and their family, as well as for colleagues.

Arbitrary detention by authorities or armed groups requires a rapid reaction: locate the person, contact the authorities, legal support, visits if possible, inform the family.

Practising and learning lessons

A crisis management team that has never practised loses precious hours. **Exercises** range from a discussion around a scenario (a 2- to 3-hour tabletop exercise) to a full simulation with real-time information injects.

A good exercise tests: activation (who calls whom, and how quickly), allocation of roles, flow of information, keeping of the log, difficult decisions (for example: whether or not to inform the media, evacuate or hibernate), and handover.

A simple indicator. Time to activate the crisis management team: target under 2 hours. During an exercise, the alert is given at 22:00; the first member is reached at 22:20, and the full team meets at 00:45: 2 hours 45 minutes, beyond the target. Cause: the contact list was out of date and two alternates had not been designated. Action: quarterly update of the list, alternates appointed, monthly call test.

After any real crisis, a **review** (after at least a few weeks) examines what worked and what needs to change, with the same learning culture as for incidents.

Exercise: the town is surrounded

Situation. Fighting is approaching a town where the organisation has 8 international staff and 54 national staff, 12 of whom come from another region and are threatened because of their ethnic group. The airport is still operating; a 14-seat aircraft (12 usable seats) can make 2 rotations a day to the capital. 4 out of 6 indicators of the "encirclement" scenario are present. The road to the capital is cut. The stocks at the main residence allow 5 days of hibernation for 20 people.

Task. 1) Hibernate, relocate or evacuate, and for whom? 2) How many days are needed to relocate the priority people by air? 3) What measures for the national staff who remain?

Answer. 1) With 4 indicators out of 6 and a road cut, the point of no return is approaching: relocate the most exposed people to the capital now (the 12 threatened staff members, with their agreement) together with non-essential international staff; keep a small essential team only if hibernation is possible and safe. 2) Priority people: 12 threatened staff + 8 international staff = 20 people, i.e. 2 rotations of 12 seats, possible in 1 day. If dependants of the threatened staff are added (for example 16 people), 36 people = 3 rotations, i.e. 2 days. 3) A salary advance of several months, daily contact through a call tree, no activity maintained without assessment and agreement, removal of organisational assets that could expose them, clear information on the options and psychological support; a plan to resume as soon as the situation allows.

Key takeaways

- Crisis management team (strategy, environment) and field team (action): terms of reference, alternates, exercises.
- First hours: activate, establish the facts, protect, inform, decide, plan; keep a log.
- Hibernate, relocate, evacuate: decide before the point of no return, on the basis of indicators.
- National staff, often the most exposed, are entitled to real options and support.
- Kidnapping: prevention, written policy, proof of life prepared, controlled communication, specialists.

Quiz

1. 30 people to relocate, aircraft with 10 usable seats. Number of rotations:
   A. 2
   B. 30
   C. 4
   D. 3

2. Hibernation of 15 people for 8 days at 4 litres of water per person per day:
   A. 120 litres
   B. 32 litres
   C. 480 litres
   D. 600 litres

3. The crisis log is mainly used to:
   A. Inform the media
   B. Keep a record of information and decisions, and facilitate handovers
   C. Appraise staff
   D. Calculate costs

4. Why prepare "proof of life" forms in advance?
   A. To verify, in the event of a kidnapping, that the person is alive, using questions to which only they know the answer
   B. For health insurance
   C. For visas
   D. For human resources

5. A crisis management team meets 3 hours 10 minutes after the alert, against a target of 2 hours. Priority action:
   A. Remove the target
   B. Do nothing, it was an exercise
   C. Change director
   D. Update contacts, designate alternates and test regularly

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

Week 8 : Health, psychosocial wellbeing, internal safeguarding and insurance

Objectives

- Organise the protection of staff health: prevention, care, medical evacuation and first aid.
- Prevent and manage stress, burnout and trauma, and measure team wellbeing.
- Treat harassment, sexual violence against staff and insurance needs as risks in their own right.

Health, the first risk

In many contexts, **illness** (malaria, digestive infections, poorly managed chronic diseases) and **accidents** cause more sick leave, repatriations and sometimes deaths than violence. Protecting health is therefore part of risk management.

Essential measures:

- **Before departure or assignment**: medical check-up, vaccinations, appropriate malaria prophylaxis, a health briefing on the context.
- **On site**: mapping of health facilities (quality, distance, opening hours, languages), contracts with clinics, first aid kits, staff trained in first aid (at least one person per team or per vehicle in isolated areas).
- **Medical evacuation**: written procedure, contract with a provider or an insurer, trigger criteria, realistic timeframes.
- **National staff**: health coverage that is equivalent in practice, including for families according to the organisation's policy.

Critical time. The "golden hour" after serious trauma is decisive. If the nearest surgical hospital is 6 hours away by road and no air evacuation is possible before the next day, the risk of a serious accident weighs much more heavily in the assessment, and advanced first aid training becomes a priority.

Stress, burnout and trauma

Aid workers are exposed to three types of stress:

- **Basic and cumulative stress**: workload, living conditions, isolation, team conflicts, permanent insecurity. Left unaddressed, it leads to **burnout**.
- **Traumatic stress**: exposure to a violent event or to death.
- **Vicarious trauma**: from repeatedly listening to and witnessing the suffering of others.

Several surveys of aid workers have found high rates of symptoms of anxiety, depression and burnout, often higher than in the general population, and higher still among national staff

exposed to the same violence as their own families.

Measures: a reasonable workload, leave and recovery breaks respected (rest and recuperation, R&R, depending on the context, for example every 6 to 12 weeks in a difficult context), confidential access to psychological support, training for managers to spot the signs, psychological first aid after an incident, a culture that does not stigmatise asking for help.

> A manager who never takes leave sends a message to the whole team. Wellbeing is also a matter of setting an example.

Measuring wellbeing

Team wellbeing is measured, like any risk:

- **Leave and R&R uptake rate**: days taken / days due.
- Average **overtime** and number of people above a threshold.
- **Sick leave** and staff turnover (early departures).
- Short, regular **anonymous surveys** (validated stress or burnout scales, questions on perceived support).
- Use of **psychological support** (in numbers, never names).

Example. A team of 40 people: 1,200 days of leave due over the year, 690 taken, i.e. 57.5%. 14 people regularly work more than 55 hours a week. Turnover: 11 departures in the year, i.e. 27.5%. These figures signal a high risk of burnout: action plan (mandatory leave planning, reinforcements, fewer meetings, follow-up by senior management).

Harassment and sexual violence against staff

Harassment (psychological and sexual), discrimination and **sexual violence** against staff, including by colleagues, are under-reported risks. They fall at once under security, human resources and internal safeguarding.

A minimum system includes:

- a clear, signed **code of conduct**, which also prohibits sexual exploitation and abuse of affected populations;
- multiple, confidential **reporting channels** (including outside the line management and external ones);
- a **survivor-centred** approach: safety, confidentiality, respect for the survivor's choices, rapid medical care (HIV post-exposure prophylaxis and emergency contraception within the time limits), psychological support;
- **investigations** conducted by trained people, independent of the line management concerned;
- effective **sanctions** and information-sharing between organisations to prevent the recruitment of sanctioned individuals (inter-agency reference-checking schemes).

Post-exposure prophylaxis kits must be available and designated staff trained in their use, because the window of effectiveness is short (ideally within the first few hours, and at the latest within 72 hours).

Insurance

Insurance transfers part of the financial risk. Usual coverage:

- **Health** (including abroad) and **medical evacuation**;
- **Accident, disability and death**, including war and terrorism risks, which are often excluded from standard policies;
- The organisation's **civil liability**;
- **Property**: vehicles, equipment, stocks, cash;
- **Kidnap and ransom**, which mainly funds specialist consultants and whose existence must remain confidential.

Points to watch: exclusions (areas, activities, war), ceilings, notification deadlines, equitable coverage of national staff, and consistency with local law (compulsory insurance).

A simple calculation. A premium of 4% of the payroll for accident and death coverage including war risks, on a payroll of USD 2,400,000: USD 96,000 a year. If the organisation insures only its 30 international staff (payroll USD 1,500,000) and leaves 120 national staff (USD 900,000) without equivalent coverage, the saving of USD 36,000 creates a serious inequality and a legal and reputational risk.

First aid and medical preparedness

Field medical preparedness is planned like everything else:

- **Training**: basic first aid for everyone, advanced first aid in isolated or conflict areas (haemorrhage control, tourniquet, recovery position, burns).
- **Equipment**: individual kit (with a tourniquet in conflict areas), vehicle kit, base kit.
- **Confidential medical records** for staff (blood group, allergies, treatments, emergency contacts), accessible only in an emergency.
- **Medical evacuation plan** for each area: first-line facility, referral facility, means of transport, timeframes, numbers, cost.

Calculating training needs. 85 staff in an isolated area, target: at least 2 people trained in advanced first aid per team of 5 on the move. If 17 teams can be in the field at the same time, at least 34 trained people are needed; with a 30% margin for absences and turnover, about 45 people.

Exercise: a team at breaking point

Situation. A base of 25 people (5 international, 20 national) in a conflict area. Over 6 months: 3 early departures of international staff, 4 long periods of sick leave among national staff; 210 days of leave taken out of 450 due; the base manager has taken no leave at all; a national staff member has told a colleague about repeated advances from a supervisor, but does not want to "make a fuss". The nearest surgical hospital is 5 hours away by road; nobody is trained in advanced first aid. The death and disability insurance covers international staff only.

Task. 1) Calculate the leave uptake rate. 2) Identify the risks. 3) Propose priority measures.

Answer. 1) 210 / 450 = 46.7%. 2) Collective burnout (little leave taken, departures and sick leave, the example set by the base manager); sexual harassment reported informally, with a risk of escalation and silence; serious medical risk (5 hours from hospital, no advanced first aider); unequal insurance coverage. 3) Mandatory planning of leave and R&R, starting with the base manager; accessible, confidential psychological support; inform the staff member, without pressuring her, of the confidential reporting channels and her options, guarantee her safety and freedom from retaliation, and involve the safeguarding function according to the policy (an alert received by a manager cannot be ignored); quickly train at least 2 people per team in advanced first aid and review the medical evacuation plan; extend the insurance to national staff.

Key takeaways

- Illness and accidents often weigh more than violence: plan prevention, care and medical evacuation.
- Cumulative, traumatic and vicarious stress: leave, R&R, confidential support, managers setting an example.
- Measure wellbeing: leave taken, hours, sick leave, turnover, anonymous surveys.
- Harassment and sexual violence: confidential channels, a survivor-centred approach, PEP within 72 hours.
- Insurance adapted to war risks, and equitable between national and international staff.

Quiz

1. A team has taken 540 days of leave out of 900 due. Uptake rate:
   A. 60%
   B. 40%
   C. 54%
   D. 90%
2. HIV post-exposure prophylaxis must be started at the latest within:
   A. 7 days
   B. 2 weeks
   C. 30 days
   D. 72 hours
3. Payroll USD 1,800,000, premium of 3%. Annual cost:
   A. USD 5,400
   B. USD 18,000
   C. USD 54,000
   D. USD 540,000
4. Vicarious trauma is caused by:
   A. A road accident
   B. Repeated exposure to the suffering of others
   C. Too much leave
   D. Jet lag
5. A manager receives an informal alert about sexual harassment. They:
   A. Inform the victim of their options and the confidential channels and activate the safeguarding procedure
   B. Wait for a written complaint
   C. Publicly confront the alleged perpetrator
   D. Ignore it if the victim does not want to make a fuss

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

Week 9 : Digital security and information protection

Objectives

- Identify the digital threats specific to humanitarian organisations: phishing, payment fraud, surveillance, data leaks.
- Put in place proportionate basic measures: authentication, backups, encryption, access management, devices.
- Protect the data of the people assisted and of staff, and respond to a digital incident.

Why digital is a security risk

Humanitarian organisations hold highly sensitive information: beneficiary lists (sometimes with biometrics and location), testimonies of violations, medical data, staff information, security analyses, movements. A leak or a hack can put **lives** in danger, not just data.

Several well-known cyberattacks have targeted humanitarian organisations, including the theft of data on hundreds of thousands of vulnerable people. Organisations are also targeted by online financial fraud and by **surveillance** of communications by state or non-state actors.

Main threats:

- **Phishing**: fake emails or messages that steal credentials or install malware.
- **Payment fraud**: a fake supplier, a fake director requesting an urgent payment, a fraudulent change of bank details.
- **Ransomware**: data encrypted in exchange for a ransom.
- **Theft or seizure of devices** (laptops, phones) at checkpoints or during robberies.
- **Surveillance** of communications and social media.
- **Internal errors**: sharing by mistake, a file sent to the wrong recipient, a password left on display.

Basic measures

A few simple measures block the vast majority of common attacks:

- **Multi-factor authentication** (MFA) on email, online storage, banking and accounting software.
- A **password manager** and long, unique passwords.
- Automatic **updates** of systems and applications.
- Regular **backups**, including one offline or isolated copy, and restore tests (3-2-1 rule: three copies, two different media, one copy off-site).
- **Encryption** of laptop and phone storage.

- **Access management**: everyone accesses only what they need; access removed on the day a staff member leaves.
- Regular **training**, with simulated phishing exercises.

Example of an exercise. A fake phishing email is sent to 120 staff: 38 click on the link (31.7%), 14 enter their credentials (11.7%), 9 report the email to the IT department (7.5%). After targeted training, a second exercise gives 12 clicks (10%), 3 credential entries (2.5%) and 41 reports (34.2%). The rise in reports is as important as the fall in clicks: it turns staff into an early warning system.

Payment fraud and financial procedures

CEO fraud and bank-detail fraud cost organisations, including humanitarian ones, considerable sums every year. Financial procedures are the best defence:

- Any **change of bank details** of a supplier or staff member is verified by calling a number already known, never the one given in the request.
- No urgent payment outside procedure, even at the apparent request of a director: dual approval remains mandatory.
- Online banking access uses dedicated devices and accounts, with dual electronic signature.
- Staff know they will be **backed** if they refuse a suspicious payment, even one requested by a superior.

> Urgency and confidentiality are fraudsters' two favourite levers: "I'm in a meeting, make this transfer right away and don't tell anyone."

Devices, checkpoints and surveillance

In the field, digital risks are also **physical**:

- At checkpoints, phones may be searched. A phone containing photos of military positions, messages critical of a party or beneficiary lists can lead to detention. Rule: carry only what is necessary, delete sensitive data from field devices, use dedicated work devices.
- Staff **social media** reveal exploitable information: real-time location, political opinions, photos of colleagues, signs of wealth. A social media policy that is explained and not punitive reduces these risks.
- End-to-end encrypted **messaging apps** protect content, but not the fact that people are communicating, nor the phone itself if it is seized unlocked.
- The use of certain tools (satellite equipment, VPNs, drones) may be prohibited or viewed with suspicion: check the legislation and acceptance.

Protecting people's data

The **data protection** of beneficiaries and staff rests on recognised principles (notably the ICRC and Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action):

- **Lawfulness and purpose**: a legitimate basis and a specific purpose for each collection.
- **Minimisation**: collect only what is necessary.
- **Informed consent** where it is the chosen basis, taking power relations into account (a household that needs aid is not free to refuse).
- **Security**: encryption, limited access, logging.
- **Limited retention** and deletion once the purpose has been fulfilled.
- **Controlled sharing** governed by data-sharing agreements, with a risk analysis (including requests from authorities or parties to the conflict).
- **Impact assessment** before any new system (biometrics, mobile payments, shared platform).

Example of minimisation. For a kit distribution, you need to identify the household and check that it has not already received the kit. Ethnic or religious affiliation is not necessary and must not be collected; a photo and fingerprint are generally not necessary either.

Responding to a digital incident

A digital incident (hacked account, stolen computer, ransomware, file sent by mistake) is handled like a security incident:

- **Contain**: change passwords, revoke sessions, isolate the infected device, remotely wipe a stolen device.
- **Assess**: what data, which people, what risk to them?
- **Inform**: senior management, the data protection officer, the people concerned if they are exposed to a risk, supervisory authorities according to the applicable law, donors according to the contracts.
- **Restore** from backups; do not pay a ransom without a decision by senior management and a legal analysis.
- **Learn**: analysis, corrections, training.

Example. An unencrypted laptop containing the list of 3,200 households with their phone numbers and locations is stolen during a robbery. The risk to the people depends on the context: if some households belong to a targeted group, it is high. Actions: immediate assessment, informing the communities concerned through safe channels if they are exposed, changing the means of contact, mandatory encryption of all laptops.

Exercise: an urgent email from the director

Situation. On a Friday at 17:00, the accountant receives an email apparently from the country director, who is travelling: "Confidential. We must pay the USD 48,000 deposit to the new fuel supplier today, otherwise we lose the contract. Bank details attached. I can't be reached, meeting with the minister." The sender's address differs by one letter from the usual address. On the same day, a regular supplier asked by email to change its bank details. The organisation's email system has no two-factor authentication.

Task. 1) Warning signs. 2) Immediate course of action. 3) Lasting measures.

Answer. 1) Urgency, confidentiality, the requester being unreachable, a new supplier with no procurement file, a slightly different sender address, a parallel request to change bank details. 2) Do not pay; call the director on their known number (or their deputy); do not change the regular supplier's details without a verification call to a number already known; report to the IT manager and to finance; keep the emails as evidence. 3) Two-factor authentication across the whole email system; a written rule: no payment outside procedure, dual approval, telephone verification of any change of bank details; training and phishing exercises; filtering of look-alike domains; a clear message from senior management: refusing a suspicious payment will always be backed.

Key takeaways

- Humanitarian data are sensitive: a leak can put lives in danger.
- MFA, unique passwords, updates, 3-2-1 backups, encryption, minimal access, training.
- Payment fraud: verification through a known number, dual approval, backing for whoever refuses.
- Field: stripped-down devices at checkpoints, a social media policy.
- Data protection: purpose, minimisation, security, limited retention, impact assessment.

Quiz

1. 150 staff receive a fake email; 24 click. Click rate:
   A. 24%
   B. 16%
   C. 6.25%
   D. 15%

2. The 3-2-1 backup rule means:
   A. 3 copies, 2 different media, 1 copy off-site
   B. 3 passwords, 2 factors, 1 account
   C. 3 days, 2 weeks, 1 month
   D. 3 servers, 2 countries, 1 cloud

3. A supplier asks by email to change its bank details. You:
   A. Change them immediately
   B. Pay in cash
   C. Reply to the email
   D. Verify by calling the number already known

4. For a kit distribution, collecting households' ethnic affiliation is:
   A. Mandatory
   B. Recommended
   C. Contrary to the minimisation principle if it is not necessary
   D. Risk-free

5. An unencrypted laptop containing beneficiary lists is stolen. First step:
   A. Buy a new laptop
   B. Assess the data exposed and the risk to the people, then inform
   C. Say nothing
   D. Publish a press release

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

Week 10 : Managing all the organisation's risks: register, appetite, compliance and reputation

Objectives

- Build and maintain an organisational risk register (security, fiduciary, operational, legal, reputational, ethical).
- Define risk appetite and translate it into thresholds and decisions, including through expected loss.
- Integrate compliance (sanctions, counter-terrorism, fraud, protection from sexual exploitation and abuse) into a single approach.

From security risks to organisational risks

Organisational risk management (often called ERM, enterprise risk management) extends the logic of security to all the risks that threaten the mission:

- **Security**: violence, accidents, staff health.
- **Fiduciary**: fraud, corruption, diversion, misuse of funds.
- **Operational**: supply disruption, partner failure, loss of access.
- **Legal and compliance**: sanctions, counter-terrorism, labour law, taxation, data protection.
- **Ethical and safeguarding**: sexual exploitation and abuse, harassment, breaches of principles.
- **Reputational**: loss of trust among communities, donors and the public.
- **Financial and strategic**: dependence on one donor, cash-flow crisis, loss of relevance.

These risks are **linked**: diversion of aid by an armed group is at once fiduciary, legal (sanctions), operational (suspension), reputational and a security issue (reprisals if the organisation denounces it). That is why an integrated approach is needed.

The risk register

The **risk register** lists the main risks, with for each one: description (cause, event, consequence), category, owner, likelihood, impact, inherent score, existing measures, residual score, additional planned measures, deadline.

Risk	Owner	Inherent	Residual	Action
Diversion of food aid by a local authority in province X	Programme director	4 × 5 = 20	3 × 4 = 12	Third-party monitoring, calls to beneficiaries, direct distribution
Fraud in fuel purchases	Finance director	4 × 3 = 12	2 × 3 = 6	Fuel cards, monthly reconciliations
Loss of the main donor (55% of income)	Executive director	3 × 5 = 15	3 × 4 = 12	Diversification plan, reserves
Sexual exploitation by a staff member or partner	Safeguarding lead	3 × 5 = 15	2 × 5 = 10	Training, reference checks, community complaints channels

The register is reviewed every quarter by senior management and every year by the board or its audit and risk committee. The **top ten risks** receive particular monitoring.

Risk appetite

Risk appetite is the level of risk the organisation is willing to take to achieve its mission. It is set by the board, by category:

- **Security**: moderate appetite, high only for life-saving activities (see programme criticality).
- **Fiduciary**: low appetite for fraud, but acceptance of a residual risk in difficult contexts, provided it is detected and reported.
- **Sexual exploitation and abuse**: zero tolerance for the behaviour, which does not prevent recognising that the risk exists and must be actively managed.
- **Programmatic**: higher appetite for innovation and for access to difficult areas.

Risk appetite is not a slogan: it is translated into **thresholds** (maximum residual score by category), **delegations** (who can accept what level of risk) and documented **decisions**. An appetite that is too low prevents work where needs are greatest; an undefined appetite leaves each manager to decide alone.

Expected loss

For some financial risks, the matrix can be supplemented by the **expected loss**: annual probability × cost if it occurs. This helps to compare the cost of a measure with the loss it avoids.

Example. Risk of theft of a field office's petty cash: estimated annual probability 20%, average loss USD 15,000 (cash and costs). Expected loss: 0.2 × 15,000 = USD 3,000 a year. Switching to mobile money payments costs USD 1,800 a year and reduces the probability to 5% and the average loss to USD 4,000: expected loss USD 200. Net gain: 3,000 − 200 − 1,800 = USD 1,000 a year, not counting the reduced security risk for the cashier.

Limits: expected loss is not suitable for risks that affect lives or whose impact is catastrophic. Nobody decides to accept a kidnapping because its "expected loss" would be low. For these risks, the reasoning is in terms of acceptable threshold and contingency plans.

Compliance: sanctions, counter-terrorism, fraud

Compliance obligations are imposed by national laws, sanctions regimes and donor contracts:

- **Sanctions and counter-terrorism**: a prohibition on making funds or resources available to listed persons or entities. Measures: screening of suppliers, partners and staff according to risk; contractual clauses; vigilance over payments in areas controlled by listed groups; use of existing humanitarian exemptions, documenting how they are applied.
- **Anti-fraud and anti-corruption**: policy, whistleblowing line, investigations, reporting to donors within deadlines (see finance).
- **Screening of end beneficiaries**: in general, donors do not require each aid recipient to be checked against the lists, and humanitarian principles are opposed to it; checks cover partners, suppliers and staff.

Dialogue with donors and banks is essential: **de-risking** by banks, which refuse to deal with organisations working in sanctioned areas, can block entire operations. Documenting one's due diligence helps to keep accounts open.

Protection from sexual exploitation and abuse

Protection from sexual exploitation and abuse (PSEA) of the people assisted is a fundamental obligation. The six core principles of the Inter-Agency Standing Committee (IASC) notably prohibit any sexual activity with children (under 18) and any exchange of money, employment, goods or services for sexual favours, and require any concern to be reported.

The system:

- code of conduct and training for all staff and partners;
- reference checks at recruitment (inter-agency schemes);
- **community-based complaints mechanisms** that are accessible, safe and adapted to women and children;
- assistance to victims (medical, psychosocial, legal) according to their choices;
- rapid and independent investigations, sanctions, reporting to donors;
- PSEA clauses in agreements with partners.

A misleading indicator: **zero complaints** does not mean zero abuse. In most contexts, the absence of complaints rather indicates that the mechanisms are neither known nor considered safe by communities.

Exercise: the board's risk committee

Situation. You present the following to an NGO's risk committee. Fuel fraud: annual probability 30%, average loss USD 25,000; proposed measure (fuel cards and reconciliations) costing USD 4,000 a year, which would reduce the probability to 10% and the loss to USD 10,000. Aid diversion in a province: inherent 4 × 5, residual 3 × 4; the board's fiduciary appetite threshold: residual ≤ 9. PSEA complaints mechanism: no complaints in 2 years across 5 provinces; a knowledge survey shows that 18% of the women interviewed know about the mechanism. A local partner has never been screened against the sanctions lists.

Task. 1) Is the fuel measure justified? 2) Is the diversion risk within appetite? What should be done? 3) What can be concluded about PSEA? 4) The partner?

Answer. 1) Current expected loss: 0.3 × 25,000 = USD 7,500; after the measure: 0.1 × 10,000 = USD 1,000; net gain: 7,500 − 1,000 − 4,000 = USD 2,500 a year: justified. 2) Residual 12 > 9: outside appetite. Options: additional measures (third-party monitoring, direct distribution, cash transfers), reduced volume in the province, or explicit, documented acceptance by the board of a temporary overrun with a plan. 3) Zero complaints with 18% awareness indicates an ineffective mechanism, not an absence of abuse: information campaign, channels adapted to women, female focal points, checking community trust. 4) Immediate screening against the sanctions lists, and systematic inclusion of this screening in the partner selection procedure.

Key takeaways

- The organisation's risks are linked: security, fiduciary, operational, legal, ethical, reputational, financial.
- A risk register with owners, inherent and residual scores, actions and deadlines, reviewed by senior management and the board.
- Risk appetite set by the board, by category, translated into thresholds and delegations.
- Expected loss = probability × cost: useful for financial risks, not for lives.
- PSEA: zero complaints is not zero abuse; sanctions: screen partners, suppliers and staff.

Quiz

1. Annual probability 25%, loss USD 12,000. Expected loss:
   A. USD 12,000
   B. USD 4,800
   C. USD 3,000
   D. USD 300
2. A measure costs USD 2,000 a year and reduces the expected loss from USD 5,000 to USD 1,500. Annual net gain:
   A. USD 3,500
   B. USD 1,500
   C. USD 5,000
   D. −USD 500
3. Who sets the organisation's risk appetite?
   A. The board
   B. Each project manager
   C. The main donor
   D. The external auditor
4. A PSEA complaints mechanism receives no complaints in two years. Most likely conclusion:
   A. There is no abuse
   B. The mechanism should be scrapped
   C. Staff are exemplary
   D. The mechanism is probably neither known nor considered safe
5. Screening against sanctions lists generally covers:
   A. Every aid recipient
   B. Journalists
   C. Partners, suppliers and staff according to risk
   D. Nobody

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

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

Week 12 : Governance, security culture, business continuity and final project

Objectives

- Organise risk governance: policy, roles of the board and senior management, reporting, audits.
- Develop a security culture in which everyone reports, learns and protects acceptance.
- Build a business continuity plan, and complete the final project: a risk management framework for a country.

The security and risk management policy

The **policy**, adopted by the board, sets the framework that all countries and departments apply:

- principles (duty of care, acceptance, right to withdraw, equal treatment, no payments to parties to the conflict);
- risk appetite and thresholds by category;
- roles and responsibilities, from senior management to focal points;
- minimum requirements: risk assessment, security plan, training, incident reporting, crisis management;
- position on sensitive issues (armed escorts, armed guards, ransoms, communication in the event of a kidnapping);
- monitoring: reports, audits, reviews.

Minimum standards by risk level make the policy operational. **Example:** in any country classified as high risk, a dedicated security adviser, a plan reviewed every 6 months, advanced training for all exposed staff, an annual crisis exercise and satellite communications in every base.

The role of the board and senior management

The **board** does not manage security day to day, but it bears ultimate responsibility for it:

- it adopts the policy and the risk appetite;
- it receives a regular report (at least annually, quarterly for major risks);
- it is informed without delay of serious incidents and crises;
- it checks that resources are sufficient and that audits are followed up.

Senior management reports using a simple dashboard: incidents by category and severity, rate per 100 staff, countries above the threshold, compliance with minimum standards (up-to-date plans, training, exercises), overdue recommendations, maturity.

Example of a reading. 12 countries; 10 have an up-to-date security plan (83%); 7 have held a crisis exercise during the year (58%); 3 countries have residual risks above the appetite. For these 3 countries, the board asks for an explicit decision: additional measures, reduced activities, or a reasoned, temporary acceptance of the overrun.

Auditing security

Security audits (internal, peer or external) check that the system exists and works:

- documents: risk assessment, plan, procedures, contact lists, incident log;
- practices: check-in calls actually made, movement logbooks, visitor registers, radio tests;
- knowledge: interviews with staff (do they know the plan, the security level, the procedure in the event of an incident?);
- equipment: condition of vehicles, communications, kits, hibernation stocks;
- equity: real measures for national staff and partners.

Sample example. The auditor interviews 30 staff: 27 know the current security level (90%), 18 know what to do if a colleague misses a check-in call (60%), 9 have taken part in an exercise during the year (30%). The written procedures exist, but ownership is weak: training and exercises become priorities.

Security culture

The best-written procedures fail without a **security culture**: a set of shared behaviours in which security is seen as a means of getting the work done, not as an obstacle.

Its signs:

- incidents and near misses are reported, and mistakes discussed without fear;
- managers follow the rules they impose;
- anyone can say "no" or "stop" without being mocked or sanctioned;
- national staff take part in analyses and decisions;
- security is discussed in programme meetings, not just among specialists;
- programme quality and personal behaviour are recognised as security measures.

> Culture shows in what happens when a manager in a hurry wants to bypass a rule. If nobody dares say anything, the security culture is weak.

Business continuity

The **business continuity plan** prepares the organisation to maintain its essential functions despite a major disruption: loss of an office, prolonged internet outage, cyberattack, pandemic, evacuation, sudden departure of key people.

Steps:

- **Identify critical functions**: payment of salaries, suppliers and transfers to beneficiaries, supply of health centres, communications with teams, donor reports falling due.
- **Set a maximum tolerable interruption for each**: for example 24 hours for emergency communications, 7 days for payroll, 30 days for donor reports.
- **Plan fallback solutions**: alternative office, remote access, backups, delegations of signing authority, back-up suppliers, stocks.
- **Designate alternates** for key functions and document essential access (without sharing passwords in plain text).
- **Test** the plan at least once a year.

Example. The payroll system is hosted on a server in the capital office. Maximum tolerable interruption: 7 days. If the office becomes inaccessible, restoring from the off-site backup takes 3 days, which is within the limit, provided the backup is recent and tested: the latest one is 5 weeks old. Action: automated daily backup, quarterly restore test.

Final project: a risk management framework for a country

The final project of the Mini MBA Security and Risk Management consists of writing, for a real country or area (using public data only, never an organisation's confidential information) or a fictitious but realistic one, a **risk management framework** of 6 to 10 pages:

- **1. Context analysis**: actors, dynamics, scenarios, indicators.
- **2. Risk assessment**: threats, vulnerabilities by profile, matrix, inherent and residual risks, comparison with the threshold.
- **3. Strategy**: mix of acceptance, protection and deterrence, and access and negotiation strategy.
- **4. Summary security plan**: levels, key procedures, communications, contingency plans (medical evacuation, hibernation, relocation, kidnapping).
- **5. People**: equitable duty of care, health, wellbeing, internal safeguarding, insurance.
- **6. Organisational risks**: extract from the register (fiduciary, compliance, PSEA, digital, reputation).
- **7. Partners, budget and governance**: risk sharing, security budget, dashboard, business continuity.

Assessment criteria: quality of the analysis, consistency between risks and measures, realism and proportionality, equity between staff and partners, respect for humanitarian principles, clarity. The project is part of the third-month exam.

Exercise: preparing the annual report to the board

Situation. Data for the year: 9 countries; 210 incidents for 1,400 staff (previous year: 168 for 1,200); serious incidents: 21 (previous year: 12); up-to-date plans in 7 countries; crisis exercises in 4 countries; 2 countries with residual risk above the appetite; 38 incident recommendations, 22 of them implemented on time; business continuity plan tested: none. Local partners reported 35 incidents, but these are not included in the official statistics.

Task. 1) Calculate the key rates and percentages. 2) What should the board take away? 3) What decisions should it be asked to take?

Answer. 1) Incident rate: 15 per 100 staff against 14 last year (+7%). Serious incident rate: 1.5 against 1.0 per 100 staff (+50%). Up-to-date plans: 7 / 9 = 78%; exercises: 4 / 9 = 44%; recommendations on time: 22 / 38 = 58%. 2) Severity is rising much faster than frequency; preparedness is insufficient (plans, exercises, continuity never tested); learning is slow; two countries are outside appetite; partners' risks are invisible in the reports. 3) Decisions: for the 2 countries outside appetite, choose between additional measures, reduced activities or reasoned, temporary acceptance; require up-to-date plans and a crisis exercise in all countries within 6 months; test the continuity plan within the year; include partners' incidents in the reports and budget for their security; monitor overdue recommendations quarterly.

Key takeaways

- A policy adopted by the board, broken down into minimum standards by risk level.
- The board bears ultimate responsibility: appetite, reports, immediate information on crises, resources.
- Audit documents, practices, knowledge, equipment and equity.
- Security culture: report without fear, be able to say stop, managers leading by example.
- Business continuity: critical functions, maximum interruption times, fallback solutions, alternates, regular tests.

Quiz

1. 9 countries, 6 with an up-to-date plan. Percentage:
   A. 67%
   B. 60%
   C. 75%
   D. 54%

2. Serious incidents: 18 for 1,200 staff. Rate per 100 staff:
   A. 18
   B. 15
   C. 0.15
   D. 1.5

3. During an audit, 12 out of 40 staff know what to do if a check-in call is missed. This indicates:
   A. Good ownership
   B. A radio problem
   C. Weak ownership (30%): training and exercises are priorities
   D. Nothing in particular

4. In a continuity plan, the maximum tolerable interruption is used to:
   A. Calculate salaries
   B. Size the fallback solutions for each critical function
   C. Appraise staff
   D. Set the communications budget

5. A strong sign of a good security culture is:
   A. Anyone can say "stop" without being sanctioned
   B. No incidents reported
   C. Very long procedures
   D. Armed guards

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