HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

Personal Security and Risk Management in the Field

Complete manual

A 2-day certified course: analysing threats, understanding acceptance, protection and deterrence strategies, applying a security plan, moving and communicating safely, and responding to common incidents, with a final assessment and a verifiable certificate. It does not replace practical Hostile Environment Awareness Training (HEAT).

https://humanitairejobs.org/en/academy/securite-terrain/

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

Contents

1. Day 1 : Understanding and managing risks
2. Day 2 : Responding to incidents and taking care of yourself
3. Day 3 : Critical incident management and the security plan

Day 1 : Understanding and managing risks

Objectives

- Calculate and reduce a risk.
- Know the three security strategies.
- Use the security plan, procedures and alert levels.

Threat, vulnerability and risk

A **threat** is anything that can cause harm (crime, fighting, explosive devices, disease, road accidents). **Vulnerability** is what exposes us to that threat (predictable schedules, a valuable vehicle, lack of communications). **Capacities** are what reduce exposure or impact (training, procedures, network of contacts).

This is often summarised as: **risk = threat × vulnerability ÷ capacities**. We can rarely act on the threat; we act mainly on our own vulnerabilities and capacities.

Important reminder: in most contexts, **road accidents** and **health problems** kill or injure more humanitarian workers than attacks do.

Acceptance, protection, deterrence

- **Acceptance**: being accepted by communities, authorities and armed groups thanks to the quality of assistance, respect for humanitarian principles (humanity, neutrality, impartiality, independence), communication and everyone's behaviour. This is the core strategy of NGOs.
- **Protection**: reducing vulnerability through physical means and procedures (walls, guards, curfews, convoys, protective vests).
- **Deterrence**: posing a counter-threat (armed escort, sanctions). NGOs use it only as a last resort, as it can compromise neutrality and acceptance.

Most organisations combine all three, with a strong emphasis on acceptance.

Security plan and procedures

Each area of operation has an up-to-date **security plan**: context and risk analysis, standard operating procedures (SOPs), contacts, medical and evacuation plans. Read it on arrival and sign it.

- **Alert levels**: each level indicates what is permitted (movements, times, areas).
- **Hibernation**: sheltering in place (office or residence) with reserves of water, food, fuel and communications for several days.
- **Relocation**: temporarily moving staff to a safer area within the country.
- **Evacuation**: moving staff out of the country. Keep a grab bag ready (documents, cash, medicines, charger).

Movements and communications

- Every movement is authorised and tracked: route, times, passengers, radio or phone check-ins at set intervals.

- Avoid routine (vary times and routes), do not drive at night unless the rules say otherwise, seat belts fastened for everyone, limited speed.
- Vehicle in good condition, full tank, first aid kit, spare wheel, contact list.
- Redundant means of communication (phone, HF/VHF radio, satellite phone) and known radio call signs.
- Seek information from NGO security forums (for example INSO where it is present) and local colleagues, who know the context best.

Conducting a security risk assessment: the complete method

The formula "risk = threat × vulnerability ÷ capacity" is a teaching starting point. In practice, a security risk assessment (*Security Risk Assessment*, SRA) is a structured, documented and regularly reviewed process that leads to decisions: which activities to maintain, under what conditions, with which measures and at what cost. The reference framework most widely used by NGOs is *Operational Security Management in Violent Environments* (Good Practice Review 8, Humanitarian Practice Network), supplemented by the guides of the Global Interagency Security Forum (GISF, formerly EISF) and, for the overall logic, by the ISO 31000 standard on risk management. United Nations agencies follow the *Security Risk Management Manual* of the Department of Safety and Security (UNDSS).

Step 1: scoping the assessment (half a day)

- **Scope**: a specific geographical area (a district, a town and its access roads), a programme or a one-off activity (a distribution, an exploratory mission). A "country-wide" assessment that is too broad does not allow decisions to be made.
- **Lead**: the country security manager or the area security focal point, under the authority of the head of mission or country director, who remains the risk owner and signs off the document.
- **Participants**: base manager, experienced drivers, logistician, at least one national staff member from each community present, programme managers. Drivers and guards are often the best informed about the real threats; leaving them out is a classic mistake.
- **Review date**: set from the outset (at least every six months, and whenever the context changes significantly).

Step 2: analysing the context (two to five days depending on access)

The context analysis answers four questions: who the actors are, what their interests are, how they perceive our organisation, and which dynamics may change over the next three to six months.

- **Actor mapping**: state authorities, security forces, non-state armed groups, customary and religious authorities, traders, local media, other humanitarian organisations. For each: interests, capacity to harm or to protect, attitude towards the organisation (favourable, neutral, hostile), existing channel of contact.
- **Incident history**: at least 12 months of data, drawn from internal reports, the NGO security forum (INSO where it operates), security coordination meetings (the UNDSS cell under *Saving Lives Together*) and the public *Aid Worker Security Database* (Humanitarian Outcomes) for regional trends.
- **Seasonal and calendar factors**: rainy season (roads cut off, isolation), lean season, transhumance, elections, religious holidays, salary payment periods (peak in robberies).

- **Perception of the organisation**: who knows us, for what, and with what image? Rumours are collected and treated as data, not as noise.

Step 3: identifying and describing threats

A threat is described precisely: perpetrator, modus operandi, usual target, place, time. "Crime" is not a usable threat; "armed robbery of 4x4 vehicles by groups of 3 to 5 men on the Kalanga-Biro road between 4 p.m. and 7 p.m., with no physical violence in 8 cases out of 10" is one. The following categories are usually distinguished:

- **Targeted threats**: the organisation or its staff are targeted as such (kidnap for ransom, retaliatory attack, written threats).
- **Opportunistic criminal threats**: staff are targeted for what they have (cash, vehicle, phone).
- **Indirect or collateral threats**: being in the wrong place at the wrong time (fighting, shelling, explosive devices, demonstrations).
- **Non-intentional threats**: road traffic accidents, illness, natural disasters, fires. In many contexts they account for the majority of staff deaths and serious injuries, yet they remain underestimated in analyses.
- **Internal threats**: fraud, internal theft, violence between colleagues, sexual harassment and exploitation, information leaks.

Step 4: assessing likelihood and impact

Each threat is rated on two scales from 1 to 5, with written definitions so that two assessors arrive at the same score.

Score	Likelihood	Impact
1	Very unlikely: no known incident of this type in the area for more than 2 years	Negligible: no injury, minor material loss, no disruption
2	Unlikely: one incident in the area in the last 12 months, not aimed at humanitarians	Minor: slight injury, loss below USD 1,000, disruption of less than 48 hours
3	Possible: several incidents over 12 months, at least one affecting a humanitarian organisation	Moderate: injury requiring treatment, loss of a vehicle, suspension of one to two weeks
4	Likely: monthly incidents, several organisations affected	Severe: serious injury, short-term abduction, one-month suspension, reputational damage
5	Very likely: weekly incidents or an explicit threat against the organisation	Critical: death, prolonged abduction, sexual violence, closure of the base

The risk level is the product of the two scores (from 1 to 25). A common convention: 1 to 4 low, 5 to 9 medium, 10 to 16 high, 20 to 25 very high (or "extreme"). What matters is that the convention is written down, known and applied consistently from one assessment to the next.

Step 5: defining measures and calculating residual risk

For each risk rated medium or above, measures are defined that act either on likelihood (avoiding exposure, making the target less attractive, improving acceptance) or on impact (first aid, insurance, response procedures, medical plan). The risk is then reassessed **with the measures in place**: this is the **residual risk**. A measure that is not budgeted, not assigned to a person and not verifiable is not a measure: it does not reduce the score.

Step 6: deciding against the risk threshold

The residual risk is compared with the organisation's **risk threshold**, i.e. the maximum level of risk it is willing to expose its staff to. This threshold is not fixed: it depends on **programme criticality**. The United Nations uses a formal *Programme Criticality Framework* that ranks activities from PC1 (immediate life-saving or directly mandated activities) to PC4; only PC1 activities can justify a very high residual risk, and only through a decision at the highest level. NGOs apply the same logic in simpler forms: water distribution in the middle of a cholera epidemic may justify a high risk; a training workshop or a donor visit does not.

> A risk assessment is not judged by the quality of the table but by the decision it produces: continue, adapt, suspend or withdraw. If the document leads to no decision and no budget line, it has served no purpose.

Step 7: disseminating, applying and reviewing

The conclusions are translated into the security plan, the standard operating procedures and the security levels. They are presented to all relevant staff, in a language they understand, during a briefing of at least one hour. A review is triggered automatically by the set review date, by a serious incident in the area, by a change in security level or by the start of a new activity.

Full example: risk assessment for opening the Kalanga base

Fictional context: the NGO "Secours Solidaire International" is preparing to open a base in Kalanga, the main town of a fictional district in the north-east of a country in protracted conflict. The project plans food and non-food item distributions for 18,000 internally displaced persons, spread between the town and three sites at 25, 40 and 65 km. The team will consist of 2 international staff, 24 national staff, 4 vehicles and a warehouse. The head of mission requests an assessment before approval by headquarters.

Data collected

- Over the last 12 months, the NGO security forum recorded 41 incidents affecting humanitarian organisations in the district: 17 armed robberies of vehicles or goods on the roads, 9 burglaries of offices or warehouses, 6 serious road traffic accidents, 4 temporary arrests of national staff at checkpoints, 3 verbal threats linked to distribution targeting, 2 short-term abductions (release in less than 72 hours), and no deaths from acts of violence.
- Two armed groups alternately control the road to the most distant site (65 km); a third, essentially criminal group operates on the 40 km road between 3 p.m. and 7 p.m.
- Rumours collected by the assessment team accuse NGOs of favouring displaced people at the expense of the host population, which has received no assistance for a year.
- The rainy season (July to October) cuts off the 65 km road for about three weeks a year.
- The district hospital has an operating theatre; the nearest hospital able to manage a polytrauma patient is in the capital, 1 hour 40 minutes away by air. The humanitarian air service (UNHAS) serves Kalanga twice a week.

Risk register (extract)

Threat	L	I	Initial risk	Main measures	L'	I'	Residual
Armed robbery of vehicle on the 40 km road (3 p.m. to 7 p.m.)	4	3	12 high	Mandatory return before 2.30 p.m.; varied departure times; no flags or stickers on valuables; no more than USD 50 in cash on board; non-resistance instruction; movement tracking with check-ins every 30 minutes	2	3	6 medium
Serious road traffic accident	3	5	15 high	Speed limiters or GPS tracking with an alert above 80 km/h; seat belts mandatory in all seats; no night driving; driver testing and training; trauma kit and a driver trained in first aid in every vehicle; maximum 10 hours of driving per day	2	4	8 medium
Warehouse burglary	4	2	8 medium	2.5 m fence, perimeter lighting, two night guards from a vetted company, key register, stock limited to 10 days of distributions	2	2	4 low
Host population hostility linked to targeting	3	4	12 high	Inclusion of 20% vulnerable host households; criteria published and explained with customary leaders; accessible complaints mechanism; balanced recruitment across communities	2	3	6 medium
Abduction of staff on the 65 km road	3	5	15 high	Prior access negotiation with both groups; national staff only, after informed consent; no international staff; day missions with no overnight stay; satellite communications; route approved the day before	2	5	10 high
Arrest of national staff at a checkpoint	3	3	9 medium	Mission orders signed by the authorities; staff ID cards; pre-established contacts with the police and gendarmerie; immediate alert procedure	2	3	6 medium
Severe malaria	4	4	16 high	Insecticide-treated nets in all accommodation; chemoprophylaxis for non-immune staff; rapid diagnostic tests and treatment at the base; medical referral plan	2	3	6 medium

Reasoning and decision

1. **Town and sites at 25 and 40 km**: all residual risks are medium at most. The head of mission approves the activities, provided the measures are budgeted and in place before the first distribution.
2. **Site at 65 km**: the residual risk of abduction remains high (10). The organisation's threshold requires approval by the regional director for any high risk, and only for life-saving activities. The team argues that 4,200 displaced people have received no food assistance for 5 months and show an estimated global acute malnutrition rate of 17%. The regional director approves for a three-month period, with monthly review, and asks for an alternative modality to be explored (mobile money transfers if the network allows, or a partnership with a local organisation that is already accepted, provided that the risk transfer is discussed openly and offset by security support).

3. **Budget**: the measures amount to USD 46,000 over 12 months (guarding, fencing, radio and satellite equipment, training, GPS tracking, insurance), i.e. 3.8% of a USD 1.2 million budget. This cost is built into the project budget as a direct cost, which most institutional donors accept when it is justified by the risk assessment.

What the example teaches

- The highest initial risk (malaria, 16) is not a risk of violence: this is often the case.
- Acceptance measures (inclusion of the host population) reduce risk as much as physical measures, at lower cost, but they involve programme teams, not just logistics.
- Relying exclusively on national staff for the most dangerous road is a **risk transfer**. It is acceptable only if national staff are genuinely less exposed (which must be demonstrated, not assumed), if they have given informed consent and if they benefit from the same protections (insurance, communications, post-incident support).

Acceptance, protection and deterrence: implementing and measuring them

The three strategies form what GPR8 calls the "security triangle". The question for a manager is not which one to choose, but how to balance the mix according to the threats: acceptance is effective against threats from actors who have an interest in our presence; it has almost no effect against opportunistic crime, explosive devices or shelling, which call for protection.

Building acceptance: an active approach

Acceptance cannot be decreed and does not flow automatically from a good programme. Joint work by several international NGOs (notably Save the Children, CARE and Mercy Corps) on acceptance-based security management formalised a five-step approach:

1. **Assess the actors**: who can harm us, protect us or influence those who can?
2. **Analyse perceptions**: how each actor perceives our mandate, our funding, our staff, our targeting criteria.
3. **Act on the factors of acceptance**: quality and relevance of aid, humanitarian principles applied and visible, fair recruitment, transparent local procurement, staff conduct, complaints handling, regular communication.
4. **Negotiate access** with those who hold power, at an appropriate level of seniority and consistently across teams.
5. **Measure and monitor** acceptance over time.

Usable acceptance indicators

Indicator	Source	Warning sign
Security information volunteered by the community (warnings, route advice)	Security focal point's log	Warnings stop, unusual silence
Unobstructed access to sites	Movement reports	Rise in refusals or demands for payment at checkpoints
Nature of complaints and rumours	Complaints mechanism, rumour tracking	Rumours of favouritism, spying or proselytism
Attendance at community meetings	Meeting minutes	Absence of leaders from a particular group
Behaviour towards off-duty national staff	Individual interviews	Pressure on families, demands for jobs under threat

A quarterly reading, recorded and compared, shows the trend. A drop in acceptance often precedes targeted incidents by several weeks.

Protection: proportionate measures

Protective measures fall into four families: **physical** (fences, lighting, access control, safe room), **procedural** (curfew, key management, movement procedures, cash management), **organisational** (training, recruitment and vetting of guards, decision-making structure) and **low profile** (unmarked vehicles, no visibility in areas where the logo attracts the threat). The main risk of heavy protection is the "bunker" effect: a fortified base sends a message of mistrust, cuts the team off from the community and can reduce acceptance.

Deterrence and armed escorts

The *IASC Non-Binding Guidelines on the Use of Armed Escorts for Humanitarian Convoys* (2013) set out the general rule: humanitarian convoys do not use armed escorts, except as a last resort, when four criteria are met: the humanitarian need is life-saving, the relevant authorities are unable to provide a secure environment, there is no alternative, and the escort itself is credible and respects international humanitarian law. The decision is documented, time-limited and reviewed. For an NGO, an armed escort raises three practical problems: it associates the organisation with a party to the conflict, it may attract attacks rather than deter them, and it sets a precedent that is hard to undo. Other, less visible forms of deterrence exist: temporary suspension of activities after an attack, coordinated withdrawal by several organisations, diplomatic representations.

> The right mix is decided threat by threat. For each line of the risk register, ask: who is the likely perpetrator, do they have an interest in our presence, and which strategy really acts on them?

Movement and communications management: detailed procedures

Travel accounts for most of the exposure of staff: the majority of robberies, abductions, attacks and accidents affecting aid workers happen on the road, according to the annual analyses of the *Aid Worker Security Database*. A written movement management procedure, applied without exception and monitored, is the most cost-effective security measure.

The movement cycle

1. **Request (the day before, by 4 p.m.)**: the requester completes a movement form: purpose, destination, main route and alternative route, departure and return times, passengers (including non-staff, who are in principle prohibited without authorisation), vehicle, driver, means of communication, planned check-in points.
2. **Approval (by 6 p.m.)**: the security focal point checks the security level of the area, the information from the last 24 hours (security forum, contact network, other organisations), the weather and road conditions. They approve, amend or refuse the movement. Movements to a high-level area are approved by the base manager or the head of mission.
3. **Pre-departure briefing (15 minutes)**: route, sensitive points, instructions at checkpoints, check-in times, conduct in the event of an incident, check of the vehicle list.
4. **Tracking (during the movement)**: the radio operator or duty officer records each check-in in the movement log: time, position, situation. Check-ins take place at departure, at each defined waypoint, on arrival, on leaving the site and on return.
5. **Closure and debrief**: on arrival, the movement is closed in the log. Any observation (new checkpoint, unusual behaviour, deteriorated road) is passed on to the focal point the same day.

The missed check-in procedure

A missed check-in is the first warning of a possible incident. The procedure must be written with precise timeframes, known to the radio operator and displayed in the radio room. Example procedure for a check-in scheduled every 30 minutes:

Time after the scheduled check-in	Action	Responsible
+ 10 minutes	Call the vehicle on all available means (VHF, HF, mobile phone, passengers' satellite phone)	Radio operator
+ 20 minutes	Inform the security focal point; check GPS tracking; call contacts along the route (another NGO, village chief, health post)	Radio operator and focal point
+ 45 minutes	Inform the base manager; freeze other movements on the same road; gather information from the security forum	Security focal point
+ 90 minutes	Activate the incident management team; inform the head of mission; decide whether or not to send a search team (never without prior assessment)	Base manager

Timeframes are shortened in high-risk areas and lengthened on roads known to have no coverage. The key point is that everyone knows in advance when the alert will be raised: a driver who knows that a missed check-in will trigger an alert after 20 minutes does not "skip" check-ins.

Communications: redundancy and discipline

- **At least two independent means** for any movement outside town: for example VHF or mobile phone plus satellite phone or HF. The satellite phone is charged, tested before departure and kept within reach, not in the boot.
- **Actual range**: VHF generally reaches 5 to 10 km in open terrain from vehicle to vehicle, more with a repeater; HF allows links over several hundred kilometres but requires a trained operator and set listening schedules.

- **Call signs and phonetic alphabet**: every person and every vehicle has a call sign; names, cash amounts or routes are never given in clear on a network that may be monitored.
- **Duress codes**: a simple code word, known to all, signals duress ("I am with guests") without alerting the perpetrators.
- **Authorisations**: the use of radios and satellite phones is subject to licensing in most countries; some prohibit or restrict them. The organisation must hold the necessary authorisations, otherwise the equipment may be seized and staff arrested.
- **Monitoring**: the radio room is staffed for the entire duration of movements and, in high-risk areas, 24 hours a day, with evening and morning radio checks for residences.

Road safety: the most underestimated threat

According to the World Health Organization, road traffic accidents are one of the leading causes of death in low- and middle-income countries, and a major cause of death and serious injury among humanitarian staff. The most effective measures are well known and inexpensive:

- Seat belts in all seats, including the rear, checked by the driver before departure (the driver has the authority to refuse to leave).
- A written maximum speed (for example 80 km/h on tarmac roads, 50 km/h on tracks, 30 km/h in villages), monitored by GPS tracking with a weekly report.
- No night driving outside town, except for an approved medical emergency.
- Limited driving time (for example 2 hours without a break, 8 to 10 hours a day) and mandatory rest.
- Driving tests on recruitment and annual driver training; no unauthorised person drives.
- Daily vehicle check against a written checklist (see the tools below) and maintenance according to the manufacturer's schedule.
- No phone use while driving, including by the vehicle team leader distracting the driver.

> A driver who refuses to leave because a passenger will not wear a seat belt, or who refuses to exceed the set speed despite pressure from a manager in a hurry, is applying the organisation's policy. Management must back them publicly, otherwise the rule will disappear within a few weeks.

Reusable tools: register, movement form and checklists

Risk register template

No.	Threat (perpetrator, modus operandi, place, time)	Target and vulnerabilities	L	I	Risk	Measures (responsible, deadline, cost)	Residual risk	Decision	Review date
1	…	…	1 to 5	1 to 5	L × I	…	…	Accepted, accepted with conditions, rejected	…

Movement form template

Section	Expected content
Purpose and justification	Activity, criticality (life-saving, important, can be postponed)
Route	Main route and alternative route, waypoints with scheduled times
Timings	Departure, arrival on site, departure from site, latest return time
People	Names, positions, phone numbers, blood group if known, emergency contact
Vehicle and driver	Registration number, radio call sign, daily check completed
Communications	Equipment carried, numbers, check-in frequency
Approval	Name of approver, date, any reservations

Daily vehicle checklist

- Fuel tank at least three-quarters full, spare jerrycan if the route requires it.
- Tyres (pressure, wear), spare wheel, jack and wheel brace.
- Brakes, headlights, indicators, windscreen wipers, horn.
- Oil and coolant.
- Complete first aid kit and trauma kit (tourniquet, pressure dressings, emergency blanket).
- In-date fire extinguisher, warning triangle, tow rope.
- Radio tested, satellite phone charged, contact list and paper map.
- Drinking water (at least 2 litres per person) and rations for an unplanned night on isolated roads.
- Vehicle documents and mission orders.

Checklist for a new staff member's arrival (first 48 hours)

1. Individual security briefing of at least one hour by the focal point, before any movement outside.
2. Reading and signing of the security plan and procedures.
3. Issue and testing of communication equipment; learning call signs and codes.
4. Site visit: residence, office, assembly point, safe room, location of the grab bag and PEP kit.
5. Recording of confidential personal data (emergency contacts, relevant medical information, proof-of-life questions).
6. Explanation of the current security level and the rules that follow from it.
7. Assignment of a buddy colleague for the first two weeks.

What donors, auditors and evaluators look at

- **ECHO**: in the Single Form, the risk and security section must show that the organisation has a security management framework, an action-specific risk analysis and budgeted measures. Justified security costs are eligible. ECHO has published a *Generic Security Guide for Humanitarian Organisations* and guidance on security within its partnership framework.
- **BHA**: the emergency application guidelines require a description of safety and security risk management, including for implementing partners.
- **FCDO and United Nations agencies**: verification of duty of care in partner due diligence assessments (risk management capacity, policies, insurance).

- **Internal auditors**: a movement log kept without gaps, signed briefing records, dated and reviewed risk assessments, incidents reported and analysed, budgeted measures actually put in place.

Common mistakes and variations by context

Common mistakes

Mistake	Consequence	How to avoid it
Copying the risk assessment from another area or a previous year	Outdated threats, unsuitable measures	Mandatory review date, incident data from the last 12 months, workshop with local staff
Describing threats in general terms ("insecurity", "crime")	Impossible to define specific measures	Describe perpetrator, modus operandi, place, time and target
Forgetting non-intentional and internal threats	The main causes of death and injury are not addressed	Mandatory headings: road, health, fire, internal threats
Assuming that national staff are less exposed	Unacknowledged risk transfer, unequal protection	Analyse the specific exposure of national staff (family pressure, community affiliation, arrests)
Unbudgeted measures	Theoretical residual risk, false sense of security	A budget line for each measure; verification during implementation
Assessment produced by a single expatriate	Bias, cultural blind spot	Participation of national staff, drivers and partners
No written risk threshold	Inconsistent decisions, pressure in the field to "go anyway"	Threshold set by senior management, linked to programme criticality

Sudden-onset and protracted crises

In the **first weeks of a sudden-onset crisis** (earthquake, mass influx of refugees, outbreak of fighting), a full assessment is impossible. A rapid assessment is carried out within 24 to 72 hours, focused on immediate threats (aftershocks, building collapses, crowds, looting, epidemics, roads), with conservative default measures (strict curfew, movements in pairs, two means of communication). The full assessment follows within 4 to 6 weeks. In a **protracted crisis**, the danger is the reverse: habit reduces vigilance, procedures become lax and the assessment is no longer reviewed. An annual audit of actual practice, compared with the written procedures, is then useful.

Camps and urban settings

In **camps**, the main threats stem from tensions between displaced people and staff (targeting, rations, recruitment), crowd movements during distributions and the possible presence of armed elements. Measures focus on how distributions are organised (separate queues, exit points, presence of committees), complaints mechanisms and coordination with camp management. In **urban settings**, crime, demonstrations, kidnapping for ransom and traffic dominate; routes and timings must be varied, a low profile is often preferable to visibility, and the security of staff residences scattered across the city becomes a major issue.

Remote management

When international or senior staff can no longer access an area, remote management transfers part of the risk to local national staff or partners. Good practice consists of acknowledging this transfer explicitly, carrying out a risk assessment specific to the staff who remain, giving those staff real authority to suspend an activity, strengthening communications and monitoring, and providing third-party monitoring mechanisms that do not expose teams any further.

Local partners with limited capacity

The Grand Bargain (2016) and the localisation commitments have increased the share of aid delivered by local organisations. These organisations are often better accepted, but less well equipped and less well insured. GISF and InterAction recommendations on partnership and security risk management stress three points: discuss risks and how they are shared openly from the partnership negotiation stage, genuinely fund the partner's security costs (equipment, training, insurance, indirect costs), and respect the partner's own analysis rather than imposing procedures designed for an international NGO.

High insecurity

In contexts of very high insecurity (active armed conflict, terrorism, frequent kidnapping of foreigners), low-profile measures often take precedence over visibility; movements are reduced to the strict minimum, international travel is limited, hibernation and relocation planning becomes a priority, and access decisions are taken at a senior level. Coordination with other actors (security forum, Saving Lives Together) becomes essential to prevent one organisation from taking on alone a risk that will expose the others.

Interview questions and key references

Security focal point, country security manager and base manager positions almost always involve a technical interview and sometimes a written exercise (risk analysis based on a scenario, drafting a procedure). Here are frequent questions and what a strong answer contains.

1. "How do you conduct a risk assessment for a new area?"

It describes a process: scoping, context and actor analysis, collection of at least 12 months of incident data, precise description of threats, defined likelihood and impact scales, budgeted and assigned measures, residual risk, decision against the risk threshold and programme criticality, dissemination and review. It mentions the participation of national staff and drivers.

2. "How do you measure acceptance?"

It cites concrete indicators (volunteered information, access, complaints and rumours, participation of leaders), regular data collection and trend analysis. It acknowledges that acceptance varies between actors and can be strong with one community and non-existent with an armed group.

3. "A programme manager wants to go ahead with a distribution despite a serious incident on the road the day before. What do you do?"

It answers neither "we cancel" nor "we go": it gathers information on the incident, reassesses the risk, looks at alternatives (48-hour postponement, another route, another modality, a local partner), applies the threshold and the written decision-making chain, and documents the decision. It points out that the programme manager cannot, alone, decide to accept a risk above the threshold.

4. "What is your view on armed escorts?"

It cites the IASC Non-Binding Guidelines on armed escorts (last resort, cumulative criteria), explains the risks to neutrality and acceptance, and offers alternatives. It acknowledges that some agencies and some contexts do use them, with documented decisions.

5. "How do you manage the security of a local partner under remote management?"

It speaks of risk sharing rather than risk transfer, assessment of the partner's capacity, funding of security costs, the right to suspend, joint training and support in the event of an incident, including insurance and psychosocial support.

6. "What was the leading cause of staff deaths in your last posting and what did you do about it?"

A strong answer is honest and backed by figures; it often cites road traffic accidents or health, and describes concrete measures (seat belts, speed, night driving, GPS tracking, driver training) with their measured effect.

Key references

- *Operational Security Management in Violent Environments*, Good Practice Review 8 (revised edition): Humanitarian Practice Network, ODI.
- *Security Risk Management: a basic guide for smaller NGOs*, *Security to go: a risk management toolkit for humanitarian aid agencies* and thematic guides: Global Interagency Security Forum (GISF, formerly EISF).
- *Security Risk Management Manual* and *Programme Criticality Framework*: United Nations Security Management System (UNDSS).
- *Saving Lives Together*: framework for security collaboration between the United Nations, NGOs and international organisations.
- *IASC Non-Binding Guidelines on the Use of Armed Escorts for Humanitarian Convoys* (2013): Inter-Agency Standing Committee.
- *Generic Security Guide for Humanitarian Organisations*: ECHO, European Commission.
- ISO 31000 standard (risk management) and ISO 31030 standard (travel risk management).
- Annual *Aid Worker Security Report* and *Aid Worker Security Database*: Humanitarian Outcomes.
- Core Humanitarian Standard on Quality and Accountability (CHS), Commitment 8 on staff support.

Exercise: risk analysis

For a regular trip made by your team (for example office → distribution site 40 km away), list three threats, rate their likelihood and impact, then propose an acceptance or protection measure for each. Then check that you know the current alert level and the hibernation procedure for your base.

Key takeaways

- Risk = threat × vulnerability ÷ capacities: we act on our vulnerabilities and capacities.
- Road accidents and health are major risks.
- Acceptance first; deterrence as a last resort.
- Hibernation (stay), relocation (within the country), evacuation (out of the country).

Quiz

1. Taking the same route at the same time every day increases:
   A. Acceptance
   B. The threat
   C. Vulnerability
   D. Capacities

2. The core security strategy of NGOs is:
   A. Armed escort
   B. Acceptance
   C. Deterrence
   D. Isolation

3. Moving staff to a safer town in the same country is called:
   A. Rotation
   B. Evacuation
   C. Relocation
   D. Hibernation

Quiz answers : 1. B · 2. B · 3. B

Day 2 : Responding to incidents and taking care of yourself

Objectives

- Know how to behave at checkpoints, in the event of carjacking or abduction.
- Respond to explosive devices and assaults.
- Report an incident and manage stress.

Checkpoints, carjacking and armed robbery

- **Checkpoint**: slow down early, switch on the interior light at night, keep hands visible, stay calm and polite, present your documents, hide nothing, take no photos, offer no money. Report your passage by radio.
- **Carjacking** or **armed robbery**: **do not resist**. Property can be replaced; lives cannot. Move slowly, announce what you are doing, hand over what is demanded, do not stare at the attackers.
- After the incident: get to safety, alert your focal point, seek medical help if necessary.

Abduction and explosive devices

Abduction: the first few minutes are the most dangerous. Do not resist, stay calm, obey simple orders, look after your health (eat, drink, move), keep a routine and keep hope. Your organisation has a crisis management procedure: trust it.

Explosive devices and explosive remnants of war (UXO, mines): stay on roads and paths that are in use; if you see a suspicious object: **do not touch**, move away by the same route, **mark** the area if it is safe to do so and **report** it to the authorities and mine action actors.

Gunfire: get down, take cover behind a solid obstacle, wait until it stops before moving.

Sexual violence and health

In the event of a sexual assault against a staff member, the organisation must offer confidential support. The HIV **post-exposure prophylaxis (PEP)** kit must be taken as soon as possible, **within 72 hours at the latest**; know where it is stored.

Health: up-to-date vaccinations, malaria prevention, safe water, known insurance and medical evacuation plan.

Reporting and taking care of yourself

Every incident, including a near miss, is **reported** promptly to your security focal point: who, what, where, when, and what was done. Reports make it possible to adjust the risk analysis for everyone; some organisations share them anonymously with security forums.

Cumulative **stress** and traumatic stress are also security risks: an exhausted professional makes poor decisions. Sleep, take breaks, stay in touch with your loved ones, talk about it, use the psychological support on offer.

To go further: the free UN online course **BSAFE** and, before a posting in a very dangerous area, practical HEAT/SSAFE training.

Checkpoints, carjacking and robbery: detailed protocols and preparation

Basic reflexes (staying calm, hands visible, non-resistance) save lives, but they are not enough for a team leader. The team leader must prepare teams before an incident, organise how each person behaves during the incident, and manage the aftermath. This section details the three most frequent situations on the road.

Checkpoints: types and reading the situation

Type of checkpoint	Indicators	Recommended conduct
Permanent official checkpoint (police, army, customs)	Consistent uniforms, fixed structure, queue of vehicles, register	Standard procedure: slow down, stop at the line, documents ready, brief and polite answers
Improvised official checkpoint	Partial uniforms, unusual hours, demand for a "contribution"	Remain courteous, politely refuse any payment by citing the organisation's policy, ask to speak to the person in charge, report by radio
Non-state armed group checkpoint	No official uniform, flags, visible weapons	Apply the negotiated access terms; show the letter or negotiation reference if one exists and if it is safe to do so; do not discuss politics
Criminal or fake checkpoint	Improvised obstacle, isolated location, men in balaclavas, no vehicles waiting	If stopping is unavoidable: total non-resistance. If the checkpoint is identified from a distance and a U-turn is possible without danger, the driver may make one according to the procedure set in advance

Checkpoint protocol, step by step

1. **On approach (200 to 300 m)**: the vehicle team leader reports the checkpoint by radio ("Alpha 2, checkpoint at point Bravo, we are approaching"); slow down gradually; dipped headlights by day, interior light on and headlights dipped at night; windows partly open; music off; sunglasses removed.
2. **When stopped**: engine running unless told otherwise; only one person speaks, usually the driver or the designated vehicle team leader; the others stay silent, hands visible.
3. **Inspection**: show the documents requested, no more; do not hand over the original passport if a certified copy is enough, unless firmly required; allow the vehicle to be searched without obstruction and observe without comment.
4. **Problematic demands**: politely refuse to carry armed persons, uniforms or goods; politely refuse to pay; if the pressure becomes threatening, give in rather than put yourself at risk, then report it.
5. **After passing through**: drive normally, without sudden acceleration; report by radio ("checkpoint passed, nothing to report" or a brief description); write a detailed report on return.

Carjacking: what happens in a few seconds

Violent vehicle theft is one of the most dangerous incidents, because perpetrators are often tense, sometimes under the influence of drugs, and react to any sudden movement. Injuries occur mainly when a victim resists, tries to escape by car or makes a gesture that is misinterpreted (reaching for a phone, unfastening a seat belt too quickly).

- **Before**: vehicles with no apparent value where possible, no visible items, doors locked in town, enough distance from the vehicle in front to manoeuvre, arrival at the residence or office with the gate opened in advance.
- **During**: stop the vehicle, put it in neutral or park, handbrake on, hands visible on the steering wheel or dashboard; announce each movement before making it ("I am unfastening my seat belt", "I am getting out"); do not stare at the perpetrators; leave the keys, engine running, and move away from the vehicle.
- **Passengers**: get out on the same side if asked, stay together, do not try to retrieve belongings, unless a child or vulnerable person is in the vehicle, in which case say so calmly.
- **After**: get to safety, check for injuries, call the base; do not pursue the perpetrators; report immediately. GPS tracking is not for pursuit, but for informing the authorities.

Armed robbery at a residence or office

A safe room (*safe room*) is only useful if the alarm is raised early enough to get there, and if it contains an independent means of communication, water and a reinforced door. If the perpetrators are already inside, non-resistance applies. A small sum of cash set aside in advance ("deterrence money", often the equivalent of USD 50 to 100) can defuse a situation, provided the organisation's policy allows it and nobody claims to have nothing.

> Non-resistance must be taught, rehearsed and backed by management. A staff member who has handed over the vehicle, cash or equipment must never be sanctioned or suspected as a matter of principle: this is how the rule is sustained.

Kidnapping, explosive devices and gunfire: understanding in order to respond better

The phases of a kidnapping

Specialists distinguish four phases, each with its own recommended conduct:

1. **Capture**: the most violent phase, lasting from a few seconds to a few minutes. The kidnappers are under stress. Do not resist, do not try to escape unless there is an obvious and safe opportunity (which is extremely rare), obey simple orders.
2. **Transport**: often long and uncomfortable (blindfolded, in a car boot, forced march). Stay calm, memorise what you can (sounds, duration, turns) without showing it, ask for water or to go to the toilet.
3. **Captivity**: from a few hours to several months. The recommendations of HEAT courses and the lessons learned from former hostages converge: establish a routine (sleep, physical exercise, hygiene), eat and drink even without appetite, keep a calm dignity, humanise your relationship with the guards without being ingratiating (talk about your family and daily life, not politics or religion), make no promises, do not lie about verifiable facts, and trust your organisation.
4. **Release or rescue**: a release can be as dangerous as the capture (transfers, confusion). In the event of an armed intervention: drop to the ground, hands visible and empty, do not run, obey

the orders of the intervention forces, who do not immediately know who is a hostage.

Preparation by the organisation

- **Proof-of-life questions**: on arrival, every exposed staff member completes three to four personal questions to which only they know the answer (for example "name of your first pet"). They are kept sealed by the crisis team and make it possible to verify that a person is alive during a negotiation.
- **Written policy**: the organisation defines in advance its position on ransoms (many organisations and several States apply a no-payment policy), who leads crisis management, the use of specialist kidnap response consultants, any insurance cover and how families will be informed.
- **Confidential information**: family contacts, the person's wishes (who to inform, who not to inform), medical information and essential treatments.

Explosive devices, landmines and explosive remnants of war

Landmines, explosive remnants of war (unexploded or abandoned ordnance) and improvised explosive devices kill and maim thousands of civilians every year and also affect humanitarian staff. The basic rules of explosive ordnance risk education, defined by the International Mine Action Standards (IMAS), are simple:

- **Before**: know the contaminated areas (maps from the United Nations Mine Action Service or the national authority), ask communities, stay on roads and paths used daily, never leave the road surface to relieve yourself or to make a U-turn on the verge in a suspect area.
- **Warning signs**: signs (often a skull and crossbones or a red triangle), stones painted red, crossed branches, abandoned fields, animal carcasses, a road suddenly avoided by local people.
- **Faced with a suspicious object**: stop, do not touch, do not approach, warn others, withdraw by exactly the same route, mark it from a distance if this can be done safely, report the precise location.
- **If a vehicle enters a minefield**: stop, do not get out, call for help, wait for deminers; if getting out is essential, reverse exactly in your own tracks.
- **Improvised explosive devices**: in affected contexts, procedures include varying routes and timings, watching for anything unusual (abandoned vehicle, new object at the roadside, wires), and sometimes safety distances from military convoys (often several hundred metres, according to local procedures).

Direct and indirect fire

- **Direct fire** (small arms, aimed fire): drop to the ground immediately, seek cover from bullets (thick wall, vehicle engine block, ditch), not just concealment from view (a car door or a bush will not stop a bullet), wait until the firing stops, move only if the cover is inadequate.
- **Indirect fire** (shells, rockets, mortars): get down, in a reinforced shelter or on the ground floor away from windows; do not go outside after the first explosion, as others often follow; wait at least 15 to 20 minutes after the last detonation, or for instructions from the base.
- **In a vehicle**: if the road ahead is blocked by gunfire, turn around if possible; if the vehicle is hit and immobilised, get out on the side away from the firing and take cover.

> These behaviours cannot be learned from a text. Before a posting to a very dangerous area, practical hostile environment training (HEAT, or SSAFE for United Nations personnel) is essential; many organisations and donors require it.

Sexual violence, medical emergencies and the medical plan

Care for a staff member who is a survivor of sexual violence

Sexual violence affects humanitarian staff, women and men, whether committed by third parties or by colleagues. The recommendations of GISF and Report the Abuse, together with WHO protocols for the clinical management of survivors, set out a survivor-centred approach: safety, confidentiality, respect for the survivor's choices, non-discrimination.

Time after the assault	Intervention	Comment
As soon as possible	Getting to safety, psychological first aid, treatment of injuries	A single trusted person, chosen by the survivor where possible
Within 72 hours at the latest	HIV post-exposure prophylaxis (PEP), 28-day course	Most effective in the first hours; no proven benefit beyond 72 hours
Up to 120 hours (5 days)	Emergency contraception	Levonorgestrel is most effective in the first 72 hours; ulipristal and the copper intrauterine device can be used up to 5 days
In the first days	Presumptive treatment of sexually transmitted infections, hepatitis B vaccination depending on status	According to the national protocol or the WHO protocol
If the person so wishes	Forensic examination, complaint to the authorities	Never imposed; the organisation provides information on the options and the risks
Follow-up	Psychological support, adjusted work arrangements, repatriation or leave if wished	Offered without any arbitrary time limit

Practical arrangements: every base has PEP kits stored at an appropriate temperature, with expiry dates checked, and at least two people trained to provide them and to refer. Staff know that the kit exists and where it is without having to ask a supervisor. Information about the incident is limited to what is strictly necessary: the security report states "serious incident against a person" without identifying details if the survivor so wishes.

The base medical plan

Every base has a written medical plan, updated every six months, which answers the following questions:

- Where are the primary, secondary and tertiary health facilities, with access times by day and by night, actual capacity (operating theatre, blood bank, radiology) and contacts?
- What means of evacuation exist: base vehicle, ambulance, humanitarian flight, the insurer's air ambulance, and with what activation times?
- Who decides on a medical evacuation and who contacts the insurer, with which phone number and which policy number?
- Who is trained in advanced first aid, and where are the trauma kits?
- What are the staff's blood groups, and is there a network of volunteer donors?

A distinction is made between **casualty evacuation** (CASEVAC, rapid transport of a casualty to the nearest facility using whatever means are available) and **medical evacuation** (MEDEVAC, medically supervised transport, often by air, organised by the insurer or a service provider). For severe trauma, the commonly used target is to reach a surgical facility within one or two hours; in many isolated contexts this is impossible, hence the importance of first aid on site: stopping bleeding (tourniquet, pressure dressing), recovery position, protection against hypothermia.

Day-to-day health

- **Malaria**: insecticide-treated nets, repellents, chemoprophylaxis for non-immune people according to medical advice, rapid diagnostic tests at the base. Any fever in an endemic area is malaria until proven otherwise.
- **Water and food**: treated water, hand hygiene, caution with raw food.
- **Vaccinations**: according to national and WHO recommendations (yellow fever, hepatitis, typhoid, pre-exposure rabies for certain postings, meningitis, cholera depending on the context).
- **Chronic conditions**: at least a three-month supply of medication for the staff concerned, with a prescription.

Reporting and analysing incidents: from flash report to trend analysis

An effective reporting system serves three purposes: triggering a rapid response (care, search, securing other teams), enabling learning (adapting procedures) and feeding into collective risk analysis (security forums). GISF and Insecurity Insight have published detailed guidance on security incident information management (*Security Incident Information Management*), which recommends a three-stage process.

The three levels of reporting

Report	Timeframe	Content	Recipients
Immediate alert (verbal, radio or phone)	As soon as the person is safe	Who, what, where, when, casualties, immediate needs	Security focal point or duty officer
Initial written report ("flash")	Within 24 hours	Known facts, action taken, needs, information still unknown	Base manager, head of mission, regional security adviser or headquarters
Full report and analysis	Within 7 days (timeframe varies between organisations)	Detailed chronology, root cause analysis, review of the response, recommendations, follow-up	Country management and headquarters; anonymised version to the security forum

Full incident report template

1. **Identification**: number, date and time, precise location (coordinates if possible), type of incident according to the organisation's classification.
2. **People involved**: position and status (national, international, partner), without sensitive health data; names only in the restricted version.
3. **Chronology**: minute-by-minute account, from departure to return to safety.
4. **Consequences**: injuries, material losses (value), disruption of activities.

5. **Response**: what was done, by whom, at what time; compliance with procedures.
6. **Analysis**: was the organisation targeted? Why this place, this time, this target? Link with previous incidents or with the programme (targeting, recruitment, dispute with a supplier)?
7. **Recommendations**: changes to procedures, the security level or the risk assessment, with a person responsible and a deadline.
8. **Follow-up**: support offered to the people concerned, insurance claims, information to the authorities, sharing with the forum.

Analysing trends

A single incident tells a story; fifty classified incidents reveal a trend. The security focal point keeps a simple database (spreadsheet) recording for each incident: date, time, location, type, presumed perpetrator, target, severity, outcome. A quarterly analysis answers specific questions: which days and times see the most robberies? Which roads? Do incidents target national or international staff, women or men more often? Are near misses increasing? This work feeds directly into the review of the risk assessment.

Why incidents go unreported

- Fear of sanctions or of being judged reckless.
- Fear of losing one's job or of seeing activities suspended (common among national staff and partners).
- Normalisation: "that checkpoint happens every day".
- Shame or fear of stigma (sexual violence, harassment).
- An overly cumbersome procedure.

> A reporting culture is built by example: systematic feedback to the person who reported, no sanctions for an incident reported in good faith, and visible changes showing that the report made a difference.

Stress, traumatic stress and team well-being

The CHS (Commitment 8) and the staff care principles of the Antares Foundation (*Managing Stress in Humanitarian Workers: Guidelines for Good Practice*) regard support for well-being as an organisational responsibility, not a private matter. Stress is not only a health issue: exhausted staff take risks, ignore procedures and communicate poorly.

Three forms of stress

Form	Causes	Signs	Response
Basic stress and cumulative stress	Workload, living conditions, isolation, team conflicts, sense of powerlessness	Persistent fatigue, irritability, sleep problems, increased alcohol consumption, cynicism, mistakes	Reasonable working hours, genuine days off, rest and recuperation periods, attentive management
Traumatic stress	Exposure to an event threatening life or physical integrity (attack, death of a colleague, sexual violence)	Acute reactions (shock, agitation, flashbacks) in the following days; most subside within a few weeks	Psychological first aid, safety, social support, referral to a professional if symptoms persist beyond 4 weeks or are disabling
Vicarious trauma and compassion fatigue	Repeated exposure to accounts of suffering (protection, GBV, mental health)	Intrusive thoughts, emotional detachment, loss of meaning	Regular clinical supervision, task rotation, peer support groups

What the organisation must put in place

- **Before departure**: selection and preparation (briefing on stress, fitness assessment if the post is highly exposed).
- **During the posting**: a reasonable workload, at least one day off per week, rest and recuperation (R&R) cycles suited to the context (often every 6 to 12 weeks in the most difficult duty stations), confidential access to psychological support, including for national staff.
- **After a critical incident**: psychological first aid (according to the WHO guide, *Psychological First Aid: Guide for Field Workers*, 2011): look, listen, link; no forced retelling of the event. Single-session psychological debriefing imposed on everyone is no longer recommended by WHO guidance on the management of acute stress.
- **At the end of the posting**: end-of-assignment interview, information on resources available after return.

The team leader's role

The manager is the first line of support. They observe changes in behaviour, hold regular one-to-one meetings, lead by example (taking their own days off), shield the team from overload imposed by headquarters or donors, and refer without diagnosing. The Inter-Agency Standing Committee Guidelines on Mental Health and Psychosocial Support in Emergency Settings (2007) point out that support for staff, national and international, is part of any response.

National staff: a frequent blind spot

National staff often live through the same events as the population (loss of family members, displacement, insecurity at home), have no rest cycle outside the area and have less access to psychological support services, which are often designed in English or French for expatriates. Good practice consists of offering services in people's own language, with trained local professionals, providing additional days off after a collective incident and involving national staff in designing support arrangements.

Full example: vehicle theft on the Moussala-Tindi road

Fictional context: the NGO "Eau et Vie" is running a water, sanitation and hygiene project in the fictional district of Moussala. On Tuesday 14 March, a vehicle leaves at 7.30 a.m. for the village of Tindi (52 km) with a driver, a national engineer and an international monitoring officer. Check-ins are scheduled every 30 minutes by satellite phone, and by VHF up to km 15.

Chronology of the incident and the response

Time	Event	Action
8.30 a.m.	Routine check-in at km 28, nothing to report	Recorded in the log
8.52 a.m.	At km 37, two motorbikes block the track; four men armed with assault rifles	The driver stops, hands on the wheel; the team applies non-resistance
9.00 a.m.	Missed check-in	The radio operator calls on all available means
9.05 a.m.	The perpetrators take the vehicle, the phones and USD 85; the team is left on the spot, uninjured	The engineer keeps a hidden mobile phone that the perpetrators overlooked
9.10 a.m.	Still no contact	The focal point is informed; GPS tracking shows the vehicle moving east, off the route
9.25 a.m.	The engineer reaches a spot with network coverage and calls the base with the agreed code "all is well, we are on foot"	Other movements on the road frozen; base manager alerted
9.40 a.m.	The base manager informs the head of mission; the village chief of Tindi offers a vehicle	Decision: the team waits in the nearest village; a second vehicle leaves the base with an experienced driver, on an approved route
11.50 a.m.	The team is back at the base	Medical check, psychological first aid, families called by the staff members themselves
2.00 p.m.	Initial report sent to headquarters	Security forum informed (anonymised version) and police notified; insurance claim filed

Analysis (full report at 7 days)

- **Target**: the vehicle (recent, highly sought-after 4x4). Three similar thefts in the district in two months, two of them against other NGOs, all between 8 a.m. and 10 a.m., on the same section of track.
- **Procedures**: non-resistance and the duress code worked; the missed check-in procedure was followed within the set timeframes. However, the previous thefts from other NGOs had been shared at the forum but not incorporated into the base's risk assessment, last reviewed seven months earlier.
- **Aggravating factors**: identical departure times for three weeks; the presence of an expatriate, which increased the value of the target; the newest vehicle in the fleet assigned to this mission.

Recommendations and follow-up

Measure	Responsible	Deadline
Review of the risk assessment for the road, with systematic monthly incorporation of forum data	Security focal point	2 weeks
Departure times varied over a 2-hour window	Logistician	Immediate
Use of less attractive or locally hired vehicles on this road	Base manager	1 month
Temporary move to the higher security level for the road (national staff only, with consent, and reassessment at 30 days)	Head of mission	Immediate
Individual follow-up meetings with the team at D+3 and D+30; referral if needed	HR manager	D+3 and D+30

What the example shows: a well-managed incident is not an incident without mistakes. The analysis revealed a systemic weakness (incorporation of external data), more significant than individual behaviour, which had been exemplary.

Common mistakes, variations and interview questions

Common mistakes

- **Immediately sending a search team** after a missed check-in, without an assessment: this risks exposing a second team to the same danger.
- **Circulating the details of an incident widely** (names, nature of an assault): breach of confidentiality, risk to the people concerned.
- **Suspecting national staff** as a matter of principle after a theft: climate of mistrust, loss of information.
- **Resuming activities without analysis** because "nobody was hurt".
- **Forgetting families**: they hear about the incident through rumour before hearing from the organisation.
- **Expired or missing PEP kits** at the moment they are needed.

Variations by context

- **Sudden-onset crisis**: health facilities may be overwhelmed or destroyed; the medical plan must be rebuilt within a few days and trauma kits reinforced.
- **Urban setting**: robberies and "express" kidnappings (forced cash machine withdrawals) are more frequent; the amount of cash and the number of bank cards carried are limited.
- **Camp**: incidents linked to distributions (crowd surges, threats) dominate; the response relies on site organisation and dialogue with committees.
- **Remote management and local partners**: the partner must have access to the same emergency arrangements (emergency fund, insurance, psychological support); otherwise the organisation transfers the risk without transferring the protection.

Interview questions

1. "A vehicle has missed its check-in for 40 minutes. Describe what you do."

A strong answer cites the missed check-in procedure with timeframes, multiple means of calling, GPS tracking, contacts along the route, freezing other movements, escalation up the management line, and an assessment before any team is sent.

2. "A colleague tells you she was sexually assaulted last night. What do you do?"

Immediate safety, non-judgemental listening, confidentiality, information on urgent care (PEP within 72 hours, emergency contraception), respect for her choices, referral according to the procedure, reporting limited to the strict minimum, follow-up. The answer avoids conducting an investigation oneself.

3. "How do you build a reporting culture?"

A simple procedure, no sanctions for good-faith reporting, systematic feedback, visible trend analysis, inclusion of near misses.

4. "How do you support a team after a serious incident?"

Psychological first aid, practical needs first, no compulsory debriefing, individual follow-up after a few days and then after one month, referral to professionals, adjusted work arrangements, particular attention to national staff.

Key references

- *Operational Security Management in Violent Environments* (GPR8): Humanitarian Practice Network.
- GISF guides on security incident information management, on managing sexual violence against aid workers and on crisis management.
- *Psychological First Aid: Guide for Field Workers* (2011): WHO, War Trauma Foundation and World Vision International.
- *Managing Stress in Humanitarian Workers: Guidelines for Good Practice*: Antares Foundation.
- IASC Guidelines on Mental Health and Psychosocial Support in Emergency Settings (2007).
- *Clinical Management of Rape and Intimate Partner Violence Survivors*: WHO, UNHCR and UNFPA.
- International Mine Action Standards (IMAS), in particular on explosive ordnance risk education.
- BSAFE online course and SSAFE training: United Nations Department of Safety and Security.

Exercise: incident report

Imagine that one of your organisation's vehicles has been stopped and robbed on a road. Write a ten-line incident report: date, time, place, people involved, sequence of events, damage, action taken, recommendations. Check where your base's PEP kit is kept and who your security focal point is.

Key takeaways

- At checkpoints: stay calm, hands visible, documents ready, no photos and no money.
- Robbery or carjacking: never resist.
- Suspicious object: do not touch, move away, mark, report.
- PEP: as soon as possible, within 72 hours at the latest.
- Every incident, even a near miss, is reported; stress is a risk to be managed.

Quiz

1. Armed men demand the keys to your vehicle. You:
   A. Hand over the keys without resisting, moving slowly
   B. Drive off at speed
   C. Refuse
   D. Negotiate at length

2. You see a suspicious metal object at the side of the path. You:
   A. Do not touch it, move away by the same route and report it
   B. Photograph it close up
   C. Pick it up to show it to someone
   D. Push it off the road

3. PEP treatment must begin:
   A. Only if symptoms appear
   B. Within the week
   C. After a month
   D. As soon as possible, at the latest 72 hours after exposure

Quiz answers : 1. B · 2. B · 3. B

Day 3 : Critical incident management and the security plan

Objectives

- Draw up a security plan and security levels.
- Manage a critical incident, from alert to lessons learned.
- Fulfil the duty of care towards all staff.

The security plan

The security plan turns the risk analysis into concrete rules: description of the context, main threats, **standard operating procedures** (movements, communications, base, cash), **security levels** (for example from 1 to 5, with the measures for each level), hibernation, relocation and evacuation plans, emergency contacts.

Everyone knows it, it is tested (drills) and revised at least every six months or after any major change. National staff, often more exposed and harder to evacuate, must be explicitly taken into account.

Managing a critical incident

A critical incident (kidnapping, attack, death, serious assault) is managed by two teams: an **incident management team** on site and a **crisis management team** at headquarters. The steps: alert, fact-finding, securing other staff, informing families through a single point of contact, controlled external communication, decisions recorded in a crisis log.

Kidnappings follow a written policy: who negotiates, with what specialist support, and within what limits. Nobody negotiates alone in the field.

Duty of care and post-incident support

The **duty of care** requires the organisation to take reasonable steps to protect its staff from foreseeable risks: information and training, equipment, insurance, procedures, psychosocial support. It applies to national and international staff alike, and to partners in a shared-risk approach.

After an incident, provide psychosocial support (psychological first aid, referral), a blame-free **lessons-learned review**, and update the security plan.

Writing a usable security plan: structure, levels and triggers

An 80-page security plan that nobody reads is an audit document, not a tool. A useful plan is short in its operational part (the procedures everyone needs to know fit into about fifteen pages), precise, and accompanied by reference annexes. The GISF guides and GPR8 propose a widely adopted structure.

Recommended structure

Part	Content	Who needs to know it
1. Introduction and validity	Area covered, date, author, approval, review date, the organisation's security policy to which the plan is linked	Everyone
2. Context and risk assessment	Summary of the context analysis, risk register, residual risks and decisions	Managers; summary for everyone
3. Security strategy	Mix of acceptance, protection and deterrence; visibility policy; relations with the authorities and armed actors	Everyone
4. Roles and responsibilities	Decision-making chain, focal point, base manager, head of mission, headquarters; responsibilities of each staff member	Everyone
5. Standard operating procedures	Movements, communications, office and residence security, cash management, visitors, information and social media, health	Everyone
6. Security levels	Description of each level, indicators for moving between levels, associated measures	Everyone
7. Incident response	Conduct by type of incident, missed check-in procedure, reporting	Everyone
8. Hibernation, relocation and evacuation plans	Triggers, locations, routes, lists of people, stocks, responsibilities	Everyone for the instructions; managers for the planning
9. Medical plan	Facilities, casualty and medical evacuation, insurance	Everyone
Annexes	Contacts, maps, radio plan, checklists, forms, grab bag list	Depending on position

Security levels: indicators, not impressions

Moving from one level to another must be based on **observable indicators** defined in advance; otherwise the decision depends on the mood of the moment and comes too late. Example of a five-level system for a fictional base:

Level	Indicators for moving to this level (examples)	Main measures	Decision
1 Normal	Stable situation, isolated criminal incidents	Standard procedures, daytime movements, 10 p.m. curfew	Base manager
2 Vigilance	Increase in incidents (more than 3 per month against NGOs in the district), political tensions, hostile rumours	8 p.m. curfew, movements outside town approved case by case, check-ins every 30 minutes, weekly review	Base manager
3 Restriction	Fighting less than 30 km away, targeted attack against a humanitarian organisation in the district, explicit threat	Essential movements only, non-essential staff prepared for relocation, hibernation stocks checked, grab bags ready	Head of mission
4 Hibernation or relocation	Fighting in town, looting, movement impossible, direct threat against the organisation	Staff gathered in hibernation locations, or relocated; activities suspended or managed remotely	Head of mission with headquarters
5 Evacuation	Collapse of law and order, likely attack on the hibernation location, airport about to close	Evacuation of the staff concerned out of the country; support for national staff who remain	Headquarters on the recommendation of the head of mission

> Returning to a lower level is also governed by written criteria (for example 14 days without a major incident in the district and confirmation by two independent sources). Without return criteria, bases remain stuck at a high level or return to normal too early.

Keeping the plan alive

- **Review** at least every six months, and after any major incident or change of level.
- **Briefing** for every new arrival, with a dated signature, and an annual refresher for all staff.
- **Exercises**: at least one hibernation or evacuation exercise per year, and a test of the alert chain (calling all staff outside working hours) every quarter.
- **Translation** into the staff's languages; a short version posted on the wall (contacts, levels, key instructions).

Hibernation, relocation and evacuation: planning for decisions made in a few hours

Decisions and their triggers

These three options are planned in calm conditions and decided under pressure. Experienced planners insist on one point: the window for leaving safely often closes faster than expected. A relocation decided too late becomes forced hibernation; an evacuation decided too late may become impossible if the airport or roads close.

Hibernation: detailed preparation

- **Location**: one or more identified buildings (office, main residence) with solid walls, an interior room without windows, a water reserve, means of communication, and the capacity to accommodate all the staff planned for.
- **Planning duration**: usually 7 to 14 days, longer in isolated areas.
- **Stocks per person per day**: at least 3 to 4 litres of water for drinking and cooking, which corresponds to the Sphere Handbook survival minimum (2.5 to 3 litres for drinking, more depending on the climate), plus water for hygiene if possible; about 2,100 kilocalories of rations requiring little or no cooking; medicines; torches and batteries; generator fuel (calculated on limited running hours, for example 4 hours a day); rubbish bags; bedding.
- **Communications**: at least two independent means, with backup power (batteries, solar panels) and a schedule of twice-daily check-ins with the capital or headquarters.
- **House rules**: stay indoors, away from windows, rotating watch, rationing, social media discipline.

Relocation and evacuation

- **Lists of people** updated every week: category (international staff, national staff from another region, local national staff, any dependants), priority, documents.
- **Main and fallback assembly points**, known to everyone, with a cut-off time.
- **Main and alternative overland routes**, with resupply points; air options (humanitarian flight, commercial flights, aircraft chartered by the insurer or by a coordination of organisations).
- **Grab bag** for each person, with limited weight (often 10 to 15 kg depending on the flights): passport and copies, cash, medicines, charger and power bank, clothes for 3 days, paper contact list.
- **Office**: list of what is taken, destroyed or left behind (sensitive documents, personal data of assisted people, cash, communications equipment).

The question of national staff

In most organisations, evacuation out of the country applies to international staff and, sometimes, to national staff whose lives are directly threatened because of their employment. Local national staff are generally not evacuated, but the organisation has obligations towards them: in-country relocation for staff from other regions, salary advances (often one to three months), means of communication, maintaining contact, clear instructions on the suspension of work, and support in the event of an individual threat. These options are discussed with staff in advance, not discovered on the day of the crisis. An evacuation that leaves national staff without instructions or resources does lasting damage to trust and acceptance.

> The day national staff are told what is planned for them must not be the day of the evacuation. This dialogue takes place on arrival, and then at each review of the plan.

Managing a critical incident: structure, roles and the first hour

A critical incident is an event that seriously threatens the life or safety of staff, or the organisation's ability to continue its activities, and that goes beyond ordinary procedures: kidnapping, disappearance, armed attack on a base, death, serious assault, arbitrary arrest, disaster affecting staff. Managing it relies on a structure activated according to written criteria and on pre-assigned roles.

Two levels of management

Team	Usual composition	Role
Incident management team (field or country)	Head of mission or country director (team leader), security manager, HR manager, a crisis log keeper; depending on the case, a doctor, a logistician	Operational management: safety of the rest of the staff, information gathering, local contacts (authorities, community), support for families on site, implementation of decisions
Crisis management team (headquarters)	Member of senior management (team leader), global security manager, HR, legal adviser, communications, and a specialist consultant where appropriate	Strategic decisions: negotiation, ransom, external communication, relations with governments, insurance, resources, liaison with families abroad

Roles to pre-assign (with deputies)

- **Team leader**: decides, arbitrates, reports. They do not take on detailed tasks themselves.
- **Crisis log keeper**: keeps the crisis log (time, information received, source, decision, who took the decision, action, person responsible). This log is essential for managing the crisis, for insurance and for any subsequent legal proceedings.
- **Family liaison officer**: the single point of contact for each family, with regular contact at agreed times, even when there is nothing new.
- **Communications lead**: the only person authorised to speak to the media, using approved messages; instructions to staff on social media.
- **Staff support lead**: teams still in the field, colleagues close to the victim, national staff.

First-hour checklist

1. Confirm the available facts and their source; distinguish what is certain from what is probable and from rumour.
2. Secure the other teams: suspend movements, recall them to the base or to a safe location, check that everyone can be reached (roll call).
3. Notify the management line according to the planned chain; activate the incident management team.
4. Open the crisis log.
5. Secure information: restricted list of people informed; instruction to stay silent on social media; retrieval of the personal data of those concerned (confidential file, proof-of-life questions).
6. Assess the medical need and activate the medical plan if necessary.
7. Decide who informs the family, when and how (never by phone from a colleague who has not been mandated; never before the facts are sufficiently established, unless there is a risk that the family will find out otherwise).
8. Inform relevant actors (security forum, Saving Lives Together coordination, embassy for international staff) in line with the organisation's policy.
9. Set the time of the next situation update (for example every 2 hours at the beginning).

Specific features of a kidnapping

Managing a kidnapping is exclusively the responsibility of the crisis management team, with specialist support. Nobody in the field negotiates on their own initiative; if the kidnappers call, the person who answers has received written instructions: listen, take notes, ask for proof of life,

promise nothing, propose a new contact at a set time and pass the information on. The first call is often decisive for what follows. Organisations that have not prepared for this situation improvise under pressure, with serious consequences (rising ransom demands, exposure of other staff members).

Death of a staff member

Procedures provide for notification of the family by a mandated person, in person if possible and accompanied; repatriation or burial according to the family's wishes and religious and legal rules; administrative and insurance formalities; support for colleagues; and a collective moment of mourning. For national staff, the organisation respects local mourning practices and provides practical support (funeral costs, allowances provided for by the contract and labour law).

Full example: 72 hours managing a disappearance in Nord-Dalé

Fictional context: the NGO "Horizons Humanitaires" works in Nord-Dalé province, where two armed groups are fighting for control of the roads. On Thursday at 2 p.m., Samuel K., a national community health worker, misses his check-in. At 3.10 p.m., his vehicle is found empty by another NGO on a secondary track, engine off, with no sign of a struggle. The driver, Joseph M., is also missing.

Extracts from the crisis log

Time	Information or decision	By	Action and person responsible
D1 2.30 p.m.	Missed check-in procedure completed without result	Security focal point	Base manager informed
D1 3.20 p.m.	Vehicle found empty at km 22 on the Bossa track	Partner NGO	Incident management team activated; all movements suspended; the 3 teams in the field recalled (return confirmed at 4.45 p.m.)
D1 4.00 p.m.	Headquarters informed; the crisis management team is activated at 5.30 p.m.	Head of mission	Crisis log opened at headquarters; first conference call at 6 p.m.
D1 6.00 p.m.	Decision: no search by the organisation; local authorities and the security forum informed; discreet request for information through the customary leaders of Bossa	Crisis team	Head of mission
D1 7.30 p.m.	Samuel's family calls the office, having been told by a villager	Family liaison officer	Visit to the family at 8 p.m. by the liaison officer and the HR manager; single contact number provided; meeting set for 10 a.m. the next day
D1 9.00 p.m.	A journalist from a local radio station asks for a statement	Communications lead	Approved statement: "We have had no news of two colleagues since this afternoon and are working with the authorities. Out of respect for them and their families, we will make no further comment."
D2 9.00 a.m.	A customary leader reports that the two men were seen with members of an armed group, apparently uninjured	Base manager	Crisis team informed; main hypothesis: detention by the group, motive unknown
D2 2.00 p.m.	Call on Samuel's phone: a man says they are being "questioned" on suspicion of spying for the rival group	Base manager (written instructions applied)	Listening, note-taking, request to speak to the two men, proposal to call back at 6 p.m.; immediate transmission
D2 6.00 p.m.	Second call; Samuel speaks for 30 seconds and correctly answers a proof-of-life question	Base manager	The crisis team appoints a single interlocutor, supported by the regional security adviser; messages: neutrality, health mission, request for unconditional release
D3 11.00 a.m.	Community and religious leaders from Bossa confirm to the group the nature of the health programme (vaccinations in	Single interlocutor	Follow-up of the mediation

Time	Information or decision	By	Action and person responsible
	villages controlled by both groups)		
D3 4.30 p.m.	Both men released at the entrance to Bossa	Base manager	Pick-up by a base vehicle; medical examination; contact with families; psychological first aid

Analysis and follow-up

- **What worked**: missed check-in procedure, rapid securing of the other teams, a single point of contact for the family, a sober media statement, written instructions for the first call, up-to-date proof-of-life questions, a network of community acceptance.
- **What was missing**: the family was informed by a villager before the organisation; the vaccination programme on both sides of the front line had not been explained to the armed group, which fuelled the suspicion of spying; no perception analysis had been carried out since the change of control of the area two months earlier.
- **Decisions**: formal access negotiation with both groups before resuming; gradual resumption after 3 weeks; psychological follow-up offered to the two colleagues and their families for 3 months; Samuel and Joseph choose their position on their return (Joseph asks for a posting in town, which is granted); review of the risk assessment and the security plan.

Duty of care: obligations, liability and post-incident support

Duty of care (*duty of care*) refers to an employer's moral and legal obligation to take reasonable measures to protect its staff against foreseeable risks. It is grounded in labour law (the employer's health and safety obligations), in the sector's quality commitments (CHS, Commitment 8) and, for travel, in the ISO 31030 (2021) standard on travel risk management.

A court ruling that left its mark on the sector

In 2015, the Oslo District Court found the Norwegian Refugee Council (NRC) grossly negligent in the case of the kidnapping of several of its staff members in the Dadaab camp (Kenya) in 2012, following a claim brought by one of them, Steve Dennis. The court noted in particular that the risks were foreseeable and that reasonable measures (such as an escort or a postponement) had not been taken. This ruling led many organisations to review their policies, how they document decisions and their insurance cover. It is a reminder that duty of care is not demonstrated by the existence of a plan, but by proof that the risks were assessed and that decisions were taken in full knowledge of the facts.

The components of a credible duty of care

Area	Minimum requirements	Expected evidence
Information	Risk briefing before departure and on arrival; informed consent for high-risk posts	Signed briefing forms
Training	Training appropriate to the level of risk (online for low-risk areas, practical hostile environment training for high-risk areas)	Training register
Procedures	Up-to-date security plan, dated and reviewed risk assessments	Signed and dated documents
Equipment	Communications, vehicles, first aid kits, protective equipment where necessary	Inventories, checks
Insurance	Health, medical evacuation, disability and death insurance, for national and international staff alike, suited to the context	Policies, certificates
Support	Psychosocial support, post-incident follow-up, support for families	Procedures, contracts with service providers
Partners	Assessment and support of security capacity, funding of costs	Partnership agreements, budgets

Equal treatment of national and international staff

Several studies by GISF and Humanitarian Outcomes have shown that national staff account for the vast majority of victims of serious incidents, while often benefiting from lesser protection (limited insurance, no evacuation, less training, inaccessible psychological support). Duty of care does not require identical measures, since the risks differ, but it does require an analysis specific to each category and measures that provide equivalent protection. An auditor or evaluator will check in particular: national staff insurance contracts, access to training, participation in the risk assessment, and the existence of options in the event of a personal threat.

Post-incident support and lessons learned

1. **Immediately**: safety, care, practical needs (accommodation, communication with loved ones), psychological first aid.
2. **In the following days**: one-to-one meeting with a trained manager; offer of professional support; information on normal reactions; adjusted work arrangements or temporary leave according to the person's wishes.
3. **At one month**: follow-up; referral to specialist care if symptoms persist.
4. **Organisational after-action review** (within 2 to 6 weeks): a structured meeting, separate from psychological support, focused on procedures and decisions, without seeking to apportion blame. Questions: what happened, what was planned, what worked, what did not work, what are we changing?
5. **Closure**: update of the plan, anonymised sharing of lessons with security forums, informing the people concerned of the changes made.

Exercises, audits, variations and interview questions

Organising a crisis simulation exercise

A 3 to 4-hour tabletop exercise (*tabletop exercise*) makes it possible to test the plan without risk. A proven method:

1. **Objectives**: two or three specific points to test (team activation, communication with families, relocation decision).
2. **Scenario**: realistic and local, divided into successive injects (for example one every 20 minutes: missed check-in, vehicle found, call from a journalist, call from the kidnappers, rumour on social media).
3. **Participants**: the actual members of the incident management team with their deputies; a facilitator from outside the team; an observer who records decisions and timings.
4. **Immediate hot debrief** (30 minutes), followed by a written report with an action plan within 2 weeks.

What a security management audit checks

Checkpoint	Frequent finding
Date of the last risk assessment	Over a year old, although the context has changed
List of people with up-to-date proof-of-life questions	Incomplete, national staff missing
Movement log	Gaps at weekends, check-ins not recorded
PEP kits	Expired or with no designated person responsible
Hibernation stocks	Water not replaced, fuel used for routine operations
Exercises	None for more than two years
National staff insurance	Limited to the minimum legal cover
Partners' security costs	Not budgeted

Variations by context

- **Sudden-onset crisis**: the plan starts as a short version (5 to 10 pages) produced in the first week: contacts, movement rules, curfew, simplified levels, assembly points, medical plan. The full version follows within the month.
- **Protracted crisis**: the risk is obsolescence; mandatory reviews are scheduled and plans are actually tested.
- **Urban setting**: scattered residences, hence more complex regrouping and hibernation plans; dependence on mobile phone networks, which can be cut.
- **Remote management**: the incident management team may be outside the country; a person on site must be designated with authority to take urgent decisions, with written delegations of authority.
- **Local partners**: plans must include partners (alerts, support in the event of an incident, access to emergency funds), and exercises can be conducted jointly.

Interview questions

1. "How do you define the indicators for moving between security levels?"

A strong answer talks about observable indicators defined in advance, linked to the threat analysis, return criteria, the decision-making chain and informing all staff. It gives an example with figures.

2. "You are head of mission; a colleague has been kidnapped. What are your priorities in the first hour?"

Safety of the other teams, confirmation of the facts, alerting the management line and activating the teams, crisis log, information management, the family, preparation for the kidnappers' first contact. The answer specifies that negotiation is the responsibility of the crisis team.

3. "What do you plan for national staff in the event of an evacuation?"

Prior dialogue, in-country relocation for staff from other regions, salary advances, communications, instructions, support in the event of a personal threat, possible evacuation when the threat is linked to their employment.

4. "What does duty of care mean to you in practice?"

The answer cites concrete, verifiable measures (information, training, procedures, insurance, support), and mentions the Dennis v. NRC ruling, equal treatment and extension to partners.

5. "How do you conduct an after-action review following a serious incident?"

Distinction between psychological support and the organisational after-action review, no search for someone to blame, structured questions, an action plan with people responsible and deadlines, feedback to the people concerned.

Key references

- *Operational Security Management in Violent Environments* (GPR8): Humanitarian Practice Network.
- GISF guides on crisis management, security planning and duty of care, including *Security to go*.
- *Security Risk Management Manual* and critical incident management procedures: UNDSS.
- ISO 31030 (2021) standard on travel risk management and ISO 31000 (2018) standard on risk management.
- Core Humanitarian Standard on Quality and Accountability (CHS), Commitment 8.
- Sphere Handbook (2018), for the minimum water and food standards used in hibernation planning.
- Humanitarian Outcomes reports (*Aid Worker Security Report*) on the exposure of national staff.
- *Managing Stress in Humanitarian Workers: Guidelines for Good Practice*: Antares Foundation.

Exercise: security levels

For a fictitious area, define four security levels (normal, vigilance, restriction, hibernation/relocation): for each, the indicators that trigger the change, movement rules, hours and communications.

Key takeaways

- Security plan: procedures, security levels, hibernation, relocation and evacuation plans.
- Critical incident: team on site + crisis team at headquarters, single point of contact for families.
- Kidnapping: written policy, nobody negotiates alone.
- Duty of care for all staff; psychosocial support and lessons learned.

Quiz

1. Who manages a kidnapping at strategic level?
   A. The crisis management team, according to the organisation's policy.
   B. The media.
   C. The family alone.
   D. The driver.

2. How often should a security plan be revised?
   A. Every ten years.
   B. At least every six months and after any major change.
   C. Only after an evacuation.
   D. Never.

3. The duty of care covers:
   A. Managers only.
   B. Consultants only.
   C. International staff only.
   D. All staff, national and international.

Quiz answers : 1. B · 2. A · 3. C