HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

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

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

A programme of exactly 3 months (12 weeks, 144 hours) to manage the security and risks of a humanitarian organisation: duty of care, context analysis, risk assessment, plans and procedures, acceptance and access negotiation, incidents, crisis management and kidnapping, staff health and wellbeing, digital security and data protection, organisational risks and compliance, risk sharing with partners, governance and business continuity. Corrected numerical exercises, three monthly exams with case studies, and a verifiable diploma from the Humanitarian Academy.

https://humanitairejobs.org/en/academy/mini-mba-securite-risques/semaine-12/

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

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

Objectives

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

The security and risk management policy

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

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

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

The role of the board and senior management

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

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

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

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

Auditing security

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

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

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

Security culture

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

Its signs:

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

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

Business continuity

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

Steps:

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

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

Final project: a risk management framework for a country

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

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

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

Exercise: preparing the annual report to the board

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

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

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

Key takeaways

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

Quiz

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

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

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

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

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

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