HUMANITARIAN ACADEMY · HUMANITAIRES JOBS

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

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

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-10/

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

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

Objectives

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

From security risks to organisational risks

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

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

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

The risk register

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

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

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

Risk appetite

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

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

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

Expected loss

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

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

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

Compliance: sanctions, counter-terrorism, fraud

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

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

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

Protection from sexual exploitation and abuse

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

The system:

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

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

Exercise: the board's risk committee

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

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

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

Key takeaways

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

Quiz

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

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