Managing security risk

Safety and security remains a major concern for humanitarian agencies with increasing levels of violence affecting aid workers.

Security Risk Management Framework

The risks of many security threats and hazards can be reduced or avoided through analysis of the context, understanding organisational vulnerability (risk assessment) and having appropriate strategies and clear plans/procedures to mitigate the risks.

1. Situation analysis and risk assessment

As a team, analyse the operating context, key actors and the impact your work could have on the context. Identify potential threats and assess risks to safety and security.

Threat / Hazard	Probability	Impact	Risk rating P x I = R	Mitigation measures
	Assess on scale of 1 – 5 (low to high)			
e.g. armed robbery	2 2	3 (on organisation) 5 (on individuals)	2 x 3 = 6 2 x 5 = 10	e.g. fencing, alarms; staff training, backups

How acceptable are those risks? For hazards or threats with a high risk rating, identify mitigation measures that need to be taken, then re-assess the likelihood and impact to determine a residual risk level. Continuously monitor and re-assess risks.

2. Security strategies – acceptance, protection, deterrence

Agencies employ a mixture of the following three strategies in order to manage, mitigate and reduce risks to safety and security. Where risks to staff are considered too high, consider options for remote management or working with local partners.

Acceptance
Build a safe operating environment through consent, approval and cooperation from individuals, communities and local authorities

Protection
Reduce risk, but not the threat by reducing the vulnerability of the organisation (e.g. fences, guards, wall)

Deterrence
Reduce risk by containing the threat with a counter threat (e.g. armed protection, diplomatic/political leverage, temporary suspension

It is important to understand that acceptance as a security strategy must be worked at and cannot be assumed just because of the work we do.

3. Security planning and procedures

Based on the strategy, write, share and practice agreed plans and procedures.

Standard Operating Procedures	Contingency plans
Agreed precautions and procedures to mitigate likelihood of threats and hazards identified, including who should do what, how and when. **e.g.** security of communication and information, office/compound, travel	Guidelines on managing security situations, including staff and resources required. Regularly review and test plans, and fully orientate all staff. **e.g.** death, injury, serious illness, kidnapping, hibernation, relocation etc.

4. Post-incident management and support

Ensure timely reporting and analysis, and support staff including psychosocial needs. Also report on near misses and include these in your analysis.

Inter-agency collaboration & information sharing

- Mutual benefit by collaborating and sharing information on security.
- Share details of specific incidents and changing security situations with other agencies.
- Any information sharing should ensure no increased risk to organisation staff affected.
- Not all agencies accept same levels of risk or have same capacity to manage risk; each agency will interpret and react to a security situation in different ways.
- Actively engage in field information exchange mechanisms, e.g:
  - informal networks
  - regular inter-agency security briefings or meetings
  - centralised security information systems such as NGO security forums.

Adapted from RedR-IHE Engineering In Emergencies

Additional resources on All In Diary web site	*Web links for further information*
Security to go: risk management toolkit © EISF 2017	INSO: http://www.ngosafety.org/
Humanitarian Security Management, HEX No 47 © ODI 2010	Security networks: EISF: http://www.eisf.eu/about/
Safety & Security Handbook © Care International 2004	INSSA: http://ingossa.org/