

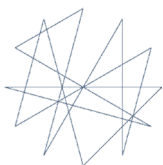
SECURITY INCIDENT INFORMATION MANAGEMENT HANDBOOK

TOOL 1: SIIM SELF-ASSESSMENT GRID



Funded by
European Union
Humanitarian Aid

eisf



redruk
people and skills for disaster relief

Aid in Danger



**Insecurity
Insight**

Data on People in Danger



TOOL 1: SIIM SELF-ASSESSMENT GRID

Please use this table as a guide to the typical elements of an incident information management system.

GENERAL QUESTIONS	
How many field/country/regional offices are currently operational in your organisation?	
Numbers of employees (international staff, national staff, volunteers, etc.)	
How many security focal points are currently working with you?	
At HQ level, are you sharing responsibility of the implementation of the security risk management framework? If yes, with whom (function)?	
SECURITY RISK MANAGEMENT FRAMEWORK	This is in place for my organisation (yes/no/partly)
Are decision-making responsibilities on security risk management clearly established at all levels?	
Does your organisation use information on the security context for other policy purposes such as advocacy, communication with donors and/or programming?	
INCIDENT AND CRISIS MANAGEMENT	
Does the organisation have an incident/crisis management policy?	
Is there an incident management framework in place at field/country level (procedures)?	
Is there an incident management framework in place at HQ level (procedures)?	
Does the incident management framework contain a communications tree?	
Does the incident management framework address near miss incidents?	
Do you train staff on incident and/or crisis management and carry out simulations?	
Is the organisation using an online incident management system?	

Is the organisation using word-processing or spreadsheet programme as the basis for its incident management system?	
Is there an agreed incident-related communications procedure with the organisation's insurance company?	
Is there a link between the security risk management policy and the HR policy in your organisation?	
COLLECTION OF INCIDENT INFORMATION	
Do you have an organisational definition of the term 'incident'?	
Does your organisation use defined categories to describe different types of incident? If so, are they standardised with the categories used by other NGOs you partner with?	
Is there an incident report template at field/country level? If yes, has it been standardised with other NGOs that you partner with?	
Is there a procedure for emotional debriefing (defusing) at field level?	
Is there a procedure for factual debriefing at field level?	
Is there a safe storage system for collected information at field level?	
Is there a safe storage system for collected information at country/regional level?	
Is there a safe storage system for collected information at HQ level?	
Does your organisation collect information on external incidents (i.e. those not impacting your organisation)?	
REPORTING AND RECORDING OF INCIDENT INFORMATION	
Is there a procedure for reporting incidents?	
Are there guidelines supporting the incident report template?	
Is there a clear reporting tree for each field office?	
Is there a list of contacts available at field/country level?	
Is there a recording system in place at field/country level?	
Is there a recording system in place at regional level?	
Is there a recording system in place at HQ level?	
Do you record loss and damage to infrastructure or equipment?	
Do you record oral, written and cyber threats to your organisation?	

Do you record administrative obstacles?	
Do you record sexual violence (including harassment) cases?	
Are incidents that are associated with sexual violence reported using the same incident management framework?	
Do you record near misses?	
Is the above system (at all levels) safe? Is data secure?	
ANALYSIS OF INCIDENT INFORMATION	
Is there a second incident reporting template providing guidance on information to be collected for analytical purposes (for example, 72 hours after the event)?	
Is someone at field/country level in charge of the analysis of an incident?	
Is someone at regional level in charge of the analysis of an incident?	
Is someone at HQ level providing analysis/verification of the regional and field/country analysis results?	
Do you train your staff to improve their analytical skills (not necessarily only on security-related topics)?	
Is there a system in place at country level to map (e.g. via spreadsheet) and analyse incidents?	
Is there some consultation of external resources (stakeholders or information) during the analysis, at field/country level?	
Is there some consultation of external resources (stakeholders or information) during the analysis, at regional level?	
Is there some consultation of external resources (stakeholders or information) during the analysis, at HQ level?	
SHARING OF INCIDENT INFORMATION	
Is there a general 'information classification' guideline or policy in the organisation?	
Is there an internal communications policy in place at field/country level?	
Is there an internal communications policy at regional level?	
Is there an internal communications policy at HQ level?	
Is the organisation part of an NGO security group at field/country level? (examples)	
Is the organisation part of an NGO security group at regional level? (examples)	
Is the organisation part of an NGO security group at HQ level? (examples)	

Is there an external communications policy at field/country level?	
Is there an external communications policy at regional level?	
Is there an external communications policy at HQ level?	
Is the organisation using social media for general communication?	
Does the organisation have established links with media stakeholders?	
Does the organisation have an actor mapping system at field/country level?	
Does the organisation have an actor mapping system at regional level?	
Does the organisation have an actor mapping system at HQ level?	
Is the tradition for internal communication oral/written?	
Is the tradition for external communication oral/written?	
Is there a field level SFP handover document including incident information?	
Are staff trained on information sharing of incidents and organisational policies?	
Do executives and board members benefit from this information sharing?	
USE OF INCIDENT INFORMATION	
Is there a person identified at field/country level in charge of follow up actions (in the mid-term)?	
Is there a follow-up communication 1 month after the incident (levels can vary)?	
Is there a follow-up communication 3 months after the incident (levels can vary)?	
Is there a follow-up of implementation of lessons learned by the HQ?	
Does your organisation do quantitative analysis?	
Does your organisation do qualitative analysis?	
Is there a system in place at country level to do quantitative data analysis on incidents?	
Is there a system in place at HQ level to do quantitative data analysis of incidents?	
Are there meetings at field level to present the data trends to staff?	

Are there meetings at country level to present the data trends to staff?	
Are there meetings at regional level to present the data trends to staff?	
Are there meetings at HQ level to present the data trends to staff?	
Are field/country SFPs consulted by programme staff?	
Is the HQ security advisor/manager consulted by programme staff?	
Are the executive and board members presented with the analysis (e.g. of trends)?	
Is data trend information shared with external stakeholders?	
Are data trends from your own organisation used in advocacy?	