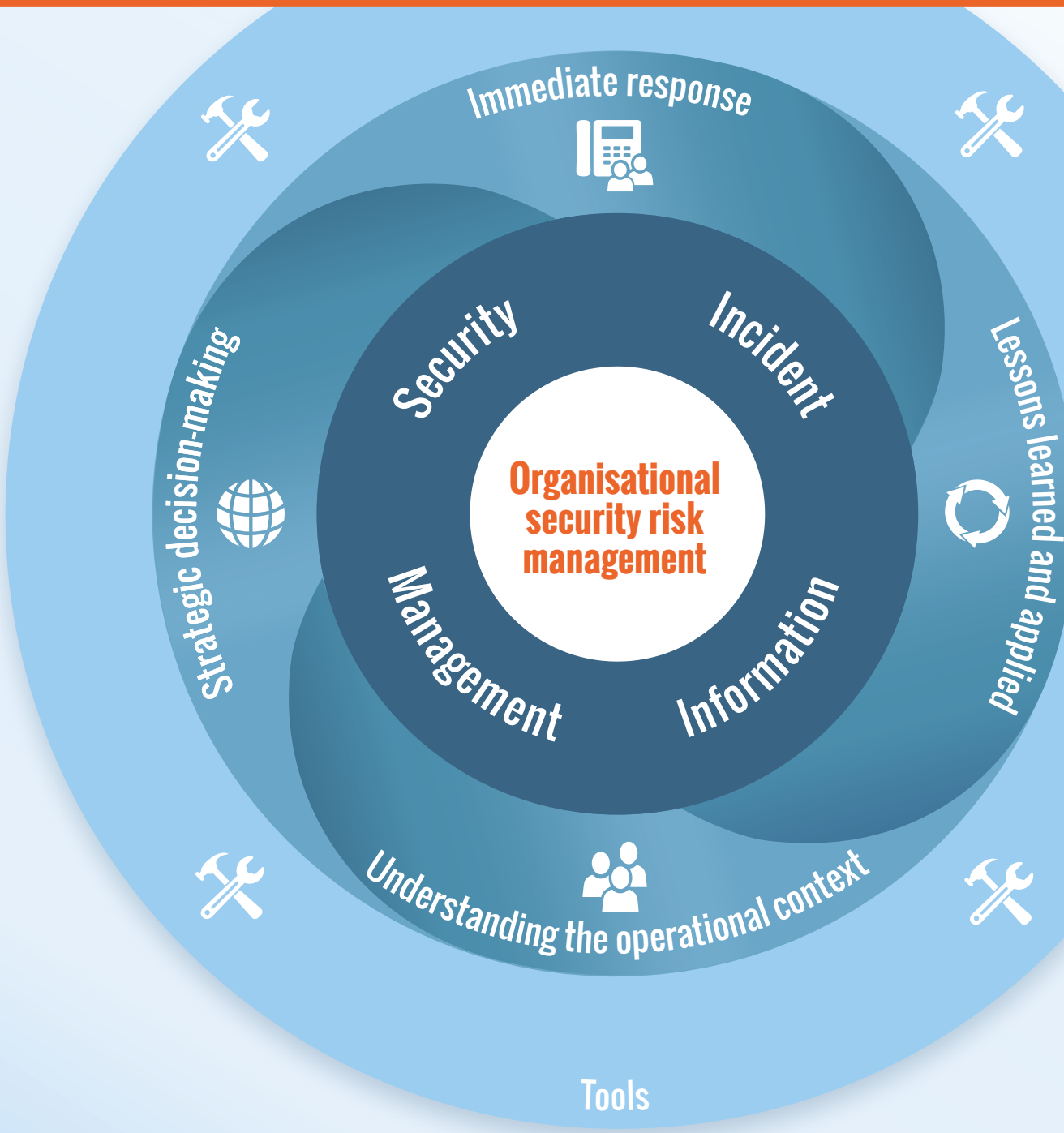
SECURITY INCIDENT INFORMATION MANAGEMENT HANDBOOK

13 TOOLS TO SUPPORT YOUR ORGANISATION



Funded by European Union Humanitarian Aid

eisf

redr uk
people and skills for disaster relief

Aid in Danger

Insecurity Insight
Data on People in Danger

This section contains guidance tools that support security incident information management. They must be read and used in conjunction with the written content of this handbook.

Tools are organised as follows (click on the item to access the tool):

- Tool 1: SIIM self-assessment grid
- Tool 2: Typology of incidents
- Tool 3: Organisational or external incident
- Tool 4: Incident reporting template
- Tool 5: Incident analysis grids
- Tool 6: How to conduct a factual debrief
- Tool 7: Good practice in gender-sensitive incident reporting and complaints mechanisms for reporting sexual exploitation and abuse (SEA)
- Tool 8: Action plan
- Tool 9: SIIM systems
- Tool 10: Incident storing
- Tool 11: Technology to report and record incidents
- Tool 12: Analysing data trends
- Tool 13: Strategic-level questions for incident management

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?	

TOOL 2: TYPOLOGY OF INCIDENTS

The following definitions of different types of incidents are given as an indication. Organisations do not have to use all the categories in their security incident information management. However, they are encouraged to use the proposed standard definitions to facilitate data exchange and cross-agency comparisons.

Incidents are defined in broad categories (such as accident, authority action, crime etc.) and associated subcategories. Agencies may choose to only use the broad categories, selected sub-categories or the broad categories and sub-categories combined.

The broad categories fulfil different functions. Some classify the event by impact (e.g. death or damage). Others describe the nature of the event (e.g. sexual violence) while others include some information on the perpetrator in addition to describing the nature of the event (e.g. crime or authority action). Others classify the context in which the event occurred (e.g. general insecurity) while other categories describe the means (e.g. use of weapons). Others classify the agency response.

It depends on the analytical focus which categorisation is the most appropriate. A single event can be considered from a variety of perspectives.

For most events, more than one of the broad categories are relevant. The subcategories can be treated as mutually exclusive, which means that only one of the subcategories usually applies.

See also the definition of event categories used in Insecurity Insight trend analysis and the data on the Humanitarian Data Exchange.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Accident Illness Natural disaster Any road traffic accidents involving staff members or agency vehicles and other incidents that were not intentional, accidents, disasters or sudden illness.	**Accident: Death**	Any unintentional death that cannot be attributed to natural causes. Causes of accidental death may include vehicle accidents, complications from injuries, etc.
	Accident: Other	A random incident that results in harm to staff and/or damage to the organisation's property.
	Accident: Vehicle	An accident involving an organisation's vehicle. Vehicle refers to any form of transportation, including, but not limited to, cars, trucks, buses, motorcycles, etc.
	Accident: Natural fire	Any fire damaging the property or endangering staff of natural or unintentional cause.
		This may include wildfires or accidental fires (such as electrical fires or gas leaks), etc.
	Illness	Any serious illness of an employee.
	Natural disaster	Actual or forecasted natural disaster that occurs, or is predicted to occur, in a city or country in which the organisation has an office. Natural disasters may include earthquakes, volcanoes, hurricanes, tornadoes, damage producing storms (hail, flash floods, etc.), floods, tsunamis, etc.
Authority action (AA) Direct or indirect actions taken by a state or non-state actor that impede the delivery of aid.	**AA: Abuse of power**	The use of legislated, executive, or otherwise authorised powers by government officials for illegitimate private gain. An illegal act by an office-holder constitutes abuse of power only if the act is directly related to their official duties.
	AA: Access denied	Acts that a) prevent an organisation from reaching beneficiaries or potential beneficiaries for needs assessments or direct service provision or acts that b) prevent beneficiaries from reaching services provided by an organisation.
	AA: Accusations	A charge by the authorities of the host country of wrongdoing.
	AA: Application of laws	Application of existing or new laws, executive orders, decrees, or regulations that, when applied, have an actual effect on the delivery of aid. This might include confiscation of equipment, putting people/organisations on watch lists, etc.
	AA: Arrest (See also Charges, detentions and imprisoned)	Arrests of staff. The arresting party must be operating in a governmental capacity (such as the police) in order to differentiate this incident from a hostage-taking incident. Arrests usually follow formal charges.
	AA: Charges	Formal legal charge made by a governmental authority asserting that a staff member or the organisation has committed a crime.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Authority action (AA) Direct or indirect actions taken by a state or non-state actor that impede the delivery of aid.	**AA: Checkpoint**	A non-border or frontier checkpoint erected in areas under military, paramilitary, or armed group control to monitor or control the movement of people and materials that impact the delivery of aid.
	AA: Denial of visa	Delay or denial of an official stamp, visa, or other permit granting permission to enter a country or territory within a country required to deliver aid.
	AA: Detention	Keeping a staff member in custody prior to official charges or without any official charges; includes temporary detention for hours or days.
	AA: Expulsion	Act of forcing a staff member or organisation to leave a country or territory.
	AA: Fine	Money that must be paid by the organisation as a punishment for not obeying a rule or law.
	AA: Forced closure	Order by government or other authorities to halt operations in a country or territory; includes closure affecting only one or multiple programmes.
	AA: Government action	Action by host or donor government that has a direct or indirect impact on the financial ability of an agency to deliver aid; includes freezing of funds, introducing taxes, or ending subsidies.
	AA: Imprisonment	Holding of a staff member in a known official or unknown location, such as a prison, often following formal charges.
	AA: Introduction of laws	Refers to the drafting or voting on laws, executive orders, decrees, or regulations that, when applied, will have a potential or actual effect on the delivery of aid. This can include, but is not limited to, restrictive registration procedures, import regulations, or regular disclosure of financial sources.
	AA: Investigation	The process or act of examining facts related to allegations against staff members or the organisation.
	AA: Property entry search	Search of a premise by external authorities.
Crime Criminally-motivated incidents that affect an agency's or staff's property.	**Crime: Armed robbery**	A robbery at gunpoint or in which the perpetrators of the robbery carried firearms that affected employees or property.
	Crime: Arson	Any fire damaging property or endangering employees that is caused intentionally. Arson includes, but is not limited to, the use of incendiary devices, the intentional sabotage of electrical systems or gas lines/tanks, and the use of an accelerant to destroy the property.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Crime Criminally-motivated incidents that affect an agency's or staff's property.	**Crime: Blackmail**	Threats, extortion or the manipulation of someone to compel them to do something; includes obtaining something, especially money, through force or threats.
	Crime: Break-in	The act of unlawfully gaining entrance into aid agency premises or vehicles, with the intention of theft.
	Crime: Burglary	Break in to a staff residence, usually with the intention of theft. Use if individuals were sleeping or otherwise unaware of the break-in.
	Crime: Carjacking/ Hijacking	Any incident in which a vehicle containing an employee(s) or owned by the organisation is forcibly seized.
	Crime: Cyber attack	Deliberate exploitation of computer systems, technology-dependent enterprises and networks resulting in disruptive consequences that can compromise data and lead to cybercrimes.
	Crime: Fraud	Wrongful or criminal deception intended to result in financial or personal gain.
	Crime: Intrusion	Wrongful or unauthorised entry into aid agency premises, vehicles or staff residences by criminals or civilians (but not state authorities).
	Crime: Looting	Theft during unrest, violence, riots or other upheavals.
	Crime: Piracy	Attacking and robbing ships at sea or boats on rivers.
	Crime: Robbery	Events in which a) the perpetrator was not armed, b) the staff member was present during the incident and fully aware of being robbed, and c) assets were taken.
	Crime: Theft of property	Any situation in which personal property is stolen from an employee or location without the crime victim being aware of the items being taken.
	Crime: Theft of organization's property	Any situation in which property (above a predefined value) is stolen from an organisation without a staff member observing how the property is taken.
	Crime: Vandalism	Deliberate destruction of or damage to agency or staff property.
Damage Any damage to agency property.	**Damage to property**	Any damage or harm, in excess of a predefined amount, that is done to the organisation's property, either unintentionally (e.g. natural disasters, accidents, and the like) or intentionally (e.g., riots that cause property damage, and the like).

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Death Any death of staff members by any cause.	**Death: Accident**	(See Accident)
	Death: Intentional (homicide)	(See KIK)
	Death: Natural	Any death that can be attributed to a natural cause, such as heart attack, illness, or stroke.
	Death: Suicide	The voluntary and intentional death of an employee by their own hand. Suicide is defined as the voluntary and intentional taking of one's own life.
General insecurity (GI) Incidents related to the general context that cause insecurity and directly or indirectly affect the delivery of aid. May or may not directly affect the agency, its staff or infrastructure.	**GI: Armed activity**	Actions involving weapons by one state, non-state, or organised armed entities.
	GI: Attack on another agency	Reported attack on another aid agency that did not affect the agency directly.
	GI: Coup	Coups, mutiny and other rebellion by any armed force. A coup is defined as an attempt (generally armed) to remove and replace a government, whether successful or not, violent or not, an attempted coup may be politically destabilising
	GI: Crossfire/active fighting	Any situation in which an employee(s) or agency property is caught in an attack or firefight between two or more armed parties. In this situation, the involved employees and properties are not the target of the attack.
	GI: Demonstration	Any demonstration (including protests, marches, sit-ins, picketing, and the like) that is nonviolent. Mass gathering of people for a political or social purpose.
	GI: Shooting	Deliberate shooting of people other than agency staff (see also KIK: homicide and WU: firearms).
	GI: Strike/no show	Deliberate decision by staff not to come to work for reasons other than illness.
	GI: Unrest	Civil or political unrest, as well as behaviour presented as tumultuous or mob-like. This behaviour includes looting, prison uprisings, crowds setting things on fire, general fighting with police (typically by protestors).
Killed, injured or kidnapped (KIK): Any incident that results in a staff member being killed, injured or kidnapped. Usually critical events.	**KIK: Abduction/hijacking/ hostage-taking/ kidnapping**	Any incident in which staff are forcibly seized. This incident may or may not involve a ransom demand.
	KIK: Beaten	Incident in which a staff member was assaulted, usually carried out with body parts (fists, feet) or objects (sticks or blunt objects).
	KIK: Death: Intentional (homicide)/killed	Any death which has been intentionally caused, for example by shooting, physical attack, poisoning, etc. Intentional deaths do not include suicides.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Killed, injured or kidnapped (KIK): Any incident that results in a staff member being killed, injured or kidnapped. Usually critical events.	**KIK: Missing**	Incident in which a staff member has disappeared or went missing. Distinction between missing and kidnapping: a) by actor: non-state actors tend to kidnap while state actors tend to 'disappear' people who are then referred to as 'missing'; b) by how the perpetrator communicates about the action that a staff member has been taken: kidnappers tend to make demands (e.g., ransom) while disappeared and missing people are usually never heard from again; c) by motive: kidnapping tends to be for a specific demand while disappearances tend to be carried out to silence a staff member, often for political reasons.
	KIK: Torture	Intentional physical maiming/injury that is explicitly characterised as torture of staff.
	KIK: Wounded	Incident in which a staff member was injured. Most injuries under wounded are inflicted with weapons as opposed to being beaten.
Motive Classification of motive of the perpetrator(s).	**Motive: Attack**	Attacks directly targeted at the agency.
	Motive: Wrong place, wrong time	Attacks that were not directed at the agency or its staff and in which staff members or agency property were affected because they happened to be near a general attack or a targeted attack against some other entity or individual.
Near miss (NM) Incidents that could have caused harm or otherwise affected the delivery of aid. Includes any situation in which a security incident almost happened but did not, happened near an aid worker/agency/programme, or where those affected were able to avoid any serious harm. (If harm results, the event is included under KIK).	**NM: Crime**	The near miss occurred in the context of a crime event.
	NM: Explosive weapons	The near miss occurred in the context of the detonation of an explosive weapon (e.g. a bombing of a neighbouring building, or a bombing at a restaurant frequented by agency staff members). Records specific events as opposed to the general use of explosive weapons in an insecure environment.
	NM: KIK	The incident narrowly avoided a staff member being killed, injured or kidnapped.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Security measures (SM) Actions taken by agencies in response to generalised insecurity or a security incident.	**SM: Evacuation: medical**	An evacuation of an employee for medical reasons, generally involving injuries or illness that cannot be treated adequately at the local hospital, doctor's office, or treatment centre.
	SM: Evacuation: non-medical	An evacuation of an employee for security reasons. Note that evacuation refers to the removal of staff from the country of operation. The shifting of staff to another location within the country for security reasons is called relocation.
	SM: Hibernation	Process of sheltering in place until the danger has passed or further assistance is rendered.
	SM: Imposed curfew	The imposition of a curfew in a city or country in which the organisation has an office.
	SM: Office closure	Decision to close an office in response to the general security context or a specific event.
	SM: Ongoing monitoring	Process of actively monitoring a security situation with a view to potentially changing the security measures.
	SM: Programme suspension	Process of significantly modifying plan activities usually by halting a specific activity or programme.
	SM: Relocation	The movement of staff to another city or office within the country of operation for security reasons.
	SM: Restricted travel, no curfew	Any restrictions on travel that affect staff. This type of event is similar to a travel advisory, and may be the result of political or social unrest, outbreaks of disease, or natural disasters.
Sexual violence Any incident in which a staff member experienced any form of sexual violence.	**Sexual violence: Aggressive sexual behaviour**	Potentially violent behaviour focussed on gratifying sexual drives.
	Sexual violence: Attempted sexual assault	Attempted act of sexual contact on the body of another person without their consent.
	Sexual violence: Rape	Sexual intercourse (oral, vaginal, or anal penetration) against the will and without the consent of the person.
	Sexual violence: Sexual assault	Act of sexual contact on the body of another person without their consent.
	Sexual violence: Unwanted sexual comments	Verbal advances that include whistling, shouting, and/or saying sexually explicit or implicit phrases or propositions that are unwanted.
	Sexual violence: Unwanted sexual touching	Touching of an unwanted sexual nature regardless of the intensity of touch. Can include massage, groping, grabbing, or grazing of any part of another person's body.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Sexual violence Any incident in which a staff member experienced any form of sexual violence.	**Sexual violence: Sexual harassment**	Unwelcome sexual advances, requests for sexual favours, and other verbal or physical conduct of a sexual nature that affects the employment of the targeted person. For example: a) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment, or b) submission to or rejection of such conduct by an individual is used as a basis for employment decisions affecting such individual, or c) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.
Threat Direct or indirect threat(s) made by a state or non-state actor that impede the delivery of aid.	**Threat: Face-to-face harassment**	Events in which a staff member is directly harassed by a person or group of people (e.g. harassment over agency's program activities or programs).
	Threat: face-to-face intimidation	Events in which a staff member is directly intimidated by a person or group of people (e.g. a staff member felt intimidated by armed actors patrolling near a food distribution).
	Threat: face-to-face threats	Events in which a staff member is directly threatened by a person or group of people; should include some form of consequence for non-compliance (e.g. a threat of retaliation for not including someone in an agency activity).
	Threat: Remote threat against agency	Events in which the agency or a staff member receives a threat not delivered face-to-face but by some remote mechanism (e.g. email, SMS, phone, or general threats issued on a website, or social media (Twitter, Facebook). Can include direct threats shouted by civilians during demonstrations.)
	Threat: reputational risk	Events involving a perceived or real, actual or potential risk to the agency's branded logo/emblem, image, or reputation.
	Threat: Threat of closure	Events involving the threat of forced closure to an activity, programme, or agency.
	Witness	Events in which a staff member witnesses an attack or crime on another staff member, family members, or beneficiaries.
Weapons use (WU) Records the type of weapon that was used in the incident, which affected staff, infrastructure or the delivery of aid.	**WU: Explosives: Aerial bombs**	Air-dropped explosive weapons, including incendiary weapons, excluding cluster bombs, and surface to surface missiles.
	WU: Explosives: Cluster bomb	Air-dropped or ground-launched explosive weapons ejecting smaller sub-munitions.
	WU: Explosives: Hand grenade	Small explosive device thrown by hand, designed to detonate after impact or after a set amount of time.

BROAD CATEGORY	SUB-CATEGORIES	DEFINITION
Weapons use (WU) Records the type of weapon that was used in the incident, which affected staff, infrastructure or the delivery of aid.	**WU: Explosives: Mines**	Any mine explosion that involves staff.
	WU: Explosives: Other	Any other explosive weapon not listed or a combination of the above.
	WU: Explosives: RCIED	Remote-controlled improvised explosive device, such as a bomb reported to have been left at the roadside and detonated when the target is near.
	WU: Explosives: Surface launched	Includes missiles, mortars, or shells that are launched from a mobile or stationary launch system, including rocket propelled grenades.
	WU: Explosives: SVIED	Person-borne improvised explosive device, e.g. explosive suicide belt, explosive in a backpack.
	WU: Explosives: VBIED	Vehicle-borne improvised explosive device, e.g. car bomb, or a car containing an explosive device.
	WU: Biological	Any use of biological weapons in a city or country in which the organisation has an office.
	WU: Chemical	Any use of chemical weapons in a city or country in which the organisation has an office.
	WU: Nuclear	Any use of nuclear weapons, both explosive and otherwise, in a city or country in which the organisation has an office.
	WU: Radiological	Any use of radiological weapons, commonly described as 'dirty bombs', in a city or country in which the organisation has an office. Possible incidents involving radiological weapons range from attacks on nuclear power plants, to attacks by improvised nuclear devices which could be constructed from stolen radiological materials.
	WU: Small arms fire	Any use of firearms or handheld weaponry which involves the organisation's employees or property.
Occupation	**Occupation of organisation's offices**	The seizure and occupation of any organisation building, warehouse, or compound by civilian or government agents.
Other	**Other incident**	An incident that cannot be adequately described by any of the pre-defined incident categories in this list. Note that if this category is selected, the reporter should provide a full description of the incident in the 'incident description' field.

TOOL 3: ORGANISATIONAL OR EXTERNAL INCIDENT

Organisations will often focus on the reporting and recording of organisational incidents (i.e. incidents that have an impact on the organisation, its staff, properties and reputation) and not include external incidents (i.e. incidents that impact other organisations) in their reporting and recording system. The organisation needs to define what constitutes an incident that affects the organisation and decide whether external incidents should be reported and recorded as well.

The below is an example of a grid developed by an organisation to help in assessing what would be considered an organisational incident and what would not. The below is subject to adaptation and changes, depending on an organisation's security policy and procedures. Please find a blank version below.

PERSON INVOLVED	WORKING HOURS		ORGANISATION GOODS IMPACTED		QUALIFICATION
	Yes	No	Yes	No	
Staff is not in-home country (international posting)	X		X		Organisational incident
	X			X	Organisational incident
		X	X		Organisational incident
		X		X	If no violence: No If with violence: Yes
Staff is in home country	X		X		Organisational incident
	X			X	Organisational incident
		X	X		Organisational incident
		X		X	Non-organisational
External stakeholder contracted by the organisation	X		X		Organisational incident
	X			X	Non-organisational
		X	X		Depending on the type of incident and goods, and the impact of the incident: yes or no
		X		X	Non-organisational

PERSON INVOLVED	WORKING HOURS		ORGANISATION GOODS IMPACTED		QUALIFICATION
	Yes	No	Yes	No	
Staff is not in-home country (international posting)					
Staff is in home country					
External stakeholder contracted by the organisation					

TOOL 4: INCIDENT REPORTING TEMPLATE

This template looks at the most immediate information needed for security incident management and preliminary analysis.

INCIDENT REFERENCE NUMBER:	
Reliability of the source and validity of information estimation[37] (according to the approved matrix):	

1. CONTACT DETAILS OF AUTHOR	
Author of the report:	Full name, position (relationship to organisation if external)
Is the author of the report the staff member involved in the incident?	Yes / No
Date of the report:	Date of submission (and version of report if not the first submission)
2. GENERAL INFORMATION ON THE INCIDENT	
Location:	Exact details on the location of the incident (including GPS coordinates if possible)
Country programme:	Exact details on the NGO programme(s) it affects
Date of the incident:	Date of the incident (if single) or detailed sequence of the incidents if multiple events
Time of the incident:	Exact time of the incident (if single) or detailed sequence/timing of the incidents if multiple events (time of the day / night)
3. CATEGORISATION OF THE INCIDENT	
Type of incident:	Intentional or accidental; Internal to the organisation or external; Hijacking; theft; robbery; extortion; road traffic accident; etc.

[37] This can be either stated at the beginning of each report or as a note within the content of the report.

4. INDICATE SEVERITY OF THE INCIDENT	
Near miss	Any situation in which a security incident almost happened but did not, or happened near an aid worker/agency/programme, or where those affected were able to avoid any serious harm.
Non-critical	People have not been physically and/or psychologically threatened. No injury.
Moderate	People have been physically and/or psychologically threatened. Minor injuries that do not require extended medical follow-up.
Serious	Serious injuries that require extended medical follow-up. Serious threat to physical and/or psychological integrity.
Lethal	A staff member of the organisation is dead as a direct consequence of the incident.
Still unknown	

5. DESCRIPTION OF THE INCIDENT
Briefly but precisely provide an overview of the event.

6. VICTIM(S)	
Full name(s):	Please indicate whether the victim is national or international staff member?
National / International staff:	What is their nationality?
Gender:	Male(s) or Female(s) or Other
Age:	How old is the victim(s)?
Other details relevant to the case:	Was the person suffering any disability or sickness that could have impacted the event?
Seniority and position in the organisation:	How long has the person been working on the programme? Position/responsibility of the victim within the organisation.
Victim's current state:	Unharmed, injured (specify the seriousness, physical or psychological) or dead.

7. WITNESSES
Indicate the full name(s) and personal contact details of the people present when the incident occurred and who can help to clarify the facts.

8. IMMEDIATE ACTION TAKEN FOLLOWING THE ACCIDENT	
Internal contacts:	Who has been informed internally about the incident (programme/mission)?
External contacts: *Donors:* *Other humanitarian/development organisations:* *Media:* *Other:*	What external authorities (local or national administrative and/or judicial, military) have been contacted following the incident?
Actions taken affecting programmes:	The incident has consequences for the programme such as the reduction of staff or the cessation of activities or the programme as a whole.
Actions taken affecting involved staff:	Follow-up/debriefing/counselling is/was necessary for staff involved in the incident.
9. PRELIMINARY ANALYSIS – RISK(S) FOR THE PROGRAMME	
Operational:	If the incident involves new risks or increases a pre-existing one for the organisation's operations, please specify.
Human Resources:	What mitigation actions were taken? If the incident involves new risks or increases a pre-existing one for the organisation's staff, please specify.
Financial/Material:	What mitigation actions were taken? If the incident involves new risks or increases a pre-existing one at the financial level or for the properties of the organisation, please specify.
Legal/Reputational:	What mitigation actions were taken? If the incident involves new risks or increases a pre-existing one at the legal level or for the image of the organisation, please specify.
Other:	What mitigation actions were taken?
10. HQ SUPPORT	
Indicate whether headquarters support is necessary and, if so, what type of support is needed.	

TOOL 5: INCIDENT ANALYSIS GRIDS

These grids will guide the analysis of impacts and causes of an incident, and how management and follow-up have been implemented during and after this initial analysis.

1. IDENTIFICATION OF THE IMPACT OF THE INCIDENT

Duration of the incident	How long did the incident last?
Type of context	According to the categorisations used in the organisation of context and type and level of violence.
Security phase	As defined in the security documents in the organisation.
Estimation of loss	
Organisation	
Money	Indicate what the direct costs of the incident have been for the organisation as a result of the incident (figures).
Equipment	Indicate if equipment/property has been damaged and its value.
Documentation	Indicate if sensitive documents (for example, list of staff) or something used to authenticate documents (for example, stamps) are missing.
Other	
Personal	
Money	Indicate the amount of cash lost by staff during the incident.
Equipment	Indicate if equipment belonging to staff has been damaged during the incident and the value.
Documentation	Indicate if personal documents belonging to the staff are missing.
Other	
Emotional Debriefing	Indicate whether an emotional debriefing has been done or not. Specify the date.

2. IDENTIFICATION OF THE CAUSES OF THE INCIDENT

POTENTIAL CONTRIBUTING FACTORS (MULTIPLE ANSWERS POSSIBLE) IS THE INCIDENT RELATED TO ...?		
Type of activity	The incident is connected to the type of work of the organisation	Specify
Lack of acceptance of our programme	The incident is the result of the lack of acceptance of the programme	Specify
Insufficient measures of protection	The incident is the result of the lack of measures of protection	Specify
Non-compliance to security rules and/or SOPs	The incident is the result of non-compliance to security rules and/or procedures	Specify
Recklessness/ lack of vigilance	The incident is the result of the recklessness or the lack of vigilance of the team	Specify
Lack of communication equipment	The incident is the result of the lack (absence or malfunction) of communication equipment necessary to the security and safety of the team	Specify
Conflict(s) within the team	The incident is the result of a conflict between two or several members of the team	Specify
Incompetence/driving of the vehicle not controlled	The incident is the result of the lack of capacity of the driver to manage the conveyance involved in the incident	Specify
Inappropriate behaviour	The incident is the result of the inappropriate behaviour of one or several members of the team (violation of the code of conduct, inappropriate clothing, etc.)	Specify
Change of context	The incident is the result of the change of the overall situation (i.e. context)	Specify
External cultural conflict	The incident is the result of pre-existing conflicts among the community such as ethnic or religious confrontations	Specify
Other	Describe unlisted factor(s) that may have contributed to the incident	

3. PATTERN IDENTIFICATION AND POTENTIAL ACTIONS

QUESTION/ PROCESS	ANSWER	POTENTIAL IMPLICATION (BASED ON ASSESSMENT)	POTENTIAL AGENCY ACTIONS
1. Has this accident happened before and how similar was it?	Yes	Accurate threat (evidenced by supporting documentation)	Communicate assessments, continue to use as basis for security decisions
	No	Flawed threat (evidenced by supporting documentation)	Change assessments and the security practices based upon them
	No	Outdated threat (evidenced by supporting documentation)	Change assessments and the security practices based upon them
2. If appropriate procedures were followed, what was the outcome?	Positive	Appropriate procedures were followed	Reinforce procedures
		Fortunate staff	Reconsider procedures
	Negative	Flawed security practices	Reconsider security practices
		High-risk propensity	Communicate to staff Train/re-train staff
3. If appropriate procedures were not followed, what was the outcome?	Positive	Inappropriate procedures	Reconsider procedures or applicability of them to all situations
		Fortunate staff	Reconsider procedures
	Negative	Lack of knowledge of procedures, possibly for the following reasons: • no security briefings for new staff; • lack of a security plan (SOPs and contingency plans); • insufficient attention to providing staff with security briefings and access to the security plan; • lack of time and encouragement for staff to read the security plan.	Consider ways to better communicate procedures to staff
		Failed at attempts to follow procedures, possibly for the following reasons: • procedures are too complicated to remember and follow; • require training that has not been provided; • require equipment that is not always available or working.	Reconsider procedures, training, equipment sufficiency
		Staff disagrees with procedures, possibly for the following reasons: • inappropriate procedures; • requirement for more training to convince staff of the importance of the procedures; • inappropriate hiring practices; • a lack of enforcement mecha-nisms within the agency.	Reconsider appropriate security-related practices

4. ANALYSIS OF THE MANAGEMENT OF THE INCIDENT

Reporting to programme managers	How successfully was information passed on? Were the organisation's time limits met?
Communications tree	How successful was the transmission of information within the field location as a whole? Did the communications tree work properly?
Roles and responsibilities	Did managers know what to do according to their responsibilities and tasks?
Pre-identification of key resource persons before the incident	Did we have clearly pre-identified key persons (externally and internally) who helped us in the management of the incident? Did we try to contact an institution/authority to help us? Did we identify the key resource person(s)? Indicate that contact person.
Communication field-HQ-field	How was the communication between HQ and the field? What do we need to improve?
Other	

TOOL 6: HOW TO CONDUCT A FACTUAL DEBRIEF

The factual debriefing process should begin after arranging for first aid or medical treatment (physical and psychological) for the involved person(s). When organising a factual debriefing for information collection purposes, it is nonetheless important to keep basic principles of psychological first aid (PFA) in mind: debriefing when basic physical and psychological security has been ensured, creating a safe space, empowering the survivor, clarity about the process, expectations and follow-up actions, etc.[38]

A factual debriefing should not be confused with an emotional debrief (also known as defusing). A traumatic event should be addressed by professionals or trained staff providing PFA.

The information below is not an attempt to train readers on PFA, or on becoming professional investigators. It is a list of tips to conduct safe and useful interviews for fact-finding, in the scope of incident reporting purposes.

When starting a factual debriefing, remind everyone involved that the purpose of the debriefing is to learn and prevent, not to find fault.

Preparing for a debriefing:

- Identify who is conducting the debrief.
- Identify who is debriefed; organisational procedures should define if the staff involved in the incident should be debriefed together or separately. The procedure can state this is a choice that is to be made on a case by case basis, depending on the event's nature and logistical constraints. While organising a collective debrief clearly presents advantages (logistical, but also for the capture of the narrative), it can also lead to the incident being 're-written' and facts altered (witnesses and victims influence each other, their perceptions vary, staff may fear giving opinions on causes and responsibilities in front of others, etc.).
- Inform the debriefed individual(s) of who is going to be present during the debriefing.
- Identify a safe space for the debriefing to take place. Pick a secure and convenient location for the individual, such as a conference room or private office.

[38] For further information on PFA, see guidelines from the World Health Organisation here.

- Allow the debriefed person to suggest the best time for the debriefing (taking other constraints into account), in line with your organisation's reporting procedures.
- Prepare your questions; questions can follow the incident reporting template and cover the same items. You might not need to ask them during the interview but they will guide you if needed. They must be open-ended questions.
- Practice self-awareness by identifying your own potential biases and putting them aside while conducting the debriefing. Analysis will come later.

Debriefing steps:

1. Conduct the interview in a quiet and private place. Put the individual at ease when they arrive and offer a glass of water, tea or coffee. Make sure they are not tired and have been emotionally debriefed.
2. State that the purpose of the debriefing is fact-finding, not fault-finding.
3. Do not promise confidentiality, but tell the individual that you will share information with only those who need to know.
4. Provide the individual with a rough estimate of the amount of time the debriefing will take.
5. Ask the individual to recount their version of what happened without interrupting. Take notes or record their responses.
6. Ask clarifying questions to fill in missing information. Use open-ended questions.
7. Recount the information obtained back to the interviewee. Correct any inconsistencies.
8. Ask the individual what they think could have prevented the incident, focusing on the conditions and events preceding the event. This can help with the analysis.
9. Avoid expressing your thoughts, opinions or conclusions about the incident or what the individual says.
10. Inform the interviewee about the next steps.
11. Thank the individual.
12. Finish documenting the debriefing by completing the incident report template.

Examples of open-ended questions:

- Where were you at the time of the incident?
- What were you doing at the time?
- What did you observe that could have been unusual?
- What did you see or hear?
- What were the environmental conditions (weather, light, noise, etc.) at the time?
- What was (were) the injured worker(s) doing at the time?
- In your opinion, what caused the incident?
- How, in your opinion, might similar incidents be prevented in the future?
- Were any other witnesses around? Do you know the names of other witnesses?
- How are you connected with others involved in the incident?
- What other details would you like to share?

What to avoid:

- Intimidating, interrupting or judging the individual.
- Assisting the individual in answering questions.
- Asking leading questions.
- Asking multiple questions at the same time.
- Becoming emotionally involved.
- Jumping to conclusions.
- Revealing discoveries of the investigation.
- Making promises that cannot be kept.

Analysis:

In order to empower the individual and give them the opportunity to share insightful comments, it is suggested you ask them for their incident analysis during the debriefing. Nonetheless, remember their judgment can be impacted by the traumatic event. The causes of the incident will have to be analysed by the person completing the incident report. The purpose of the fact-finding debriefing is to determine all the contributing factors to why the incident occurred.

The following questions may help in your analysis of the contributing factors:

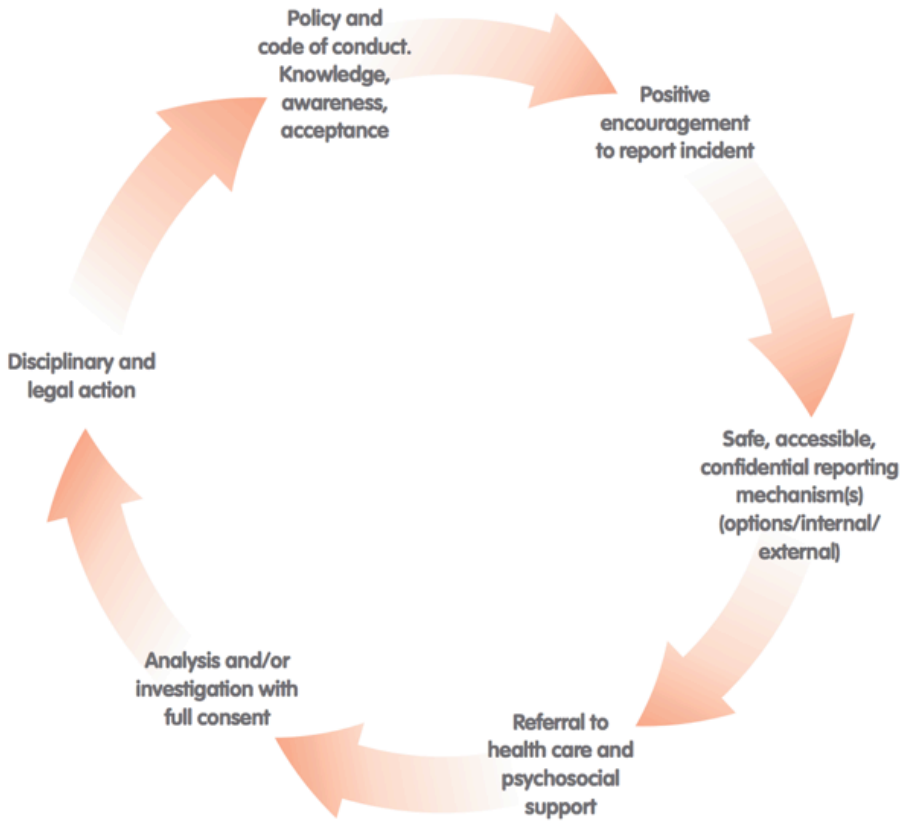
- Was a hazardous condition a contributing factor?
- Was the location a contributing factor?
- Was the procedure a contributing factor?
- Was lack of personal protective equipment or emergency equipment a contributing factor?
- Were the SOPs a contributing factor, and should they be updated to reflect a new reality on the ground?
- Were the team dynamics a contributing factor, and how do you feel we could improve this?

Statements such as 'staff were careless' or 'the employee did not follow safety procedures', 'wrong time, wrong place' do not get at the root cause of an incident. To avoid these misleading conclusions, focus on why the incident occurred, e.g. 'Why did the employee not follow safety procedures?'

TOOL 7: GOOD PRACTICE IN GENDER-SENSITIVE INCIDENT REPORTING & COMPLAINTS MECHANISMS FOR REPORTING SEA

This tool offers a summary of good practices in reporting and follow-up of gender sensitive incidents and SEA. This should guide organisations in developing and adapting their systems.

Sensitive incidents reporting cycle[39]



[39] This tool is extracted from Persaud, C. (2012). *Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management*. EISF.

Policy:
Policy is at the foundation of good incident reporting and may include a whistleblowing clause. Special emphasis should be placed on promoting incident reporting. There should be mandatory reporting for specific incidents, except situations where it is an option for an individual, such as incidents of harassment and gender-based violence (GBV). (Sexual exploitation and abuse (SEA) falls under a different code of conduct and policy. Staff members have a duty to report incidents of sexual exploitation and abuse or possibly face disciplinary measures. See below for more information.)

Awareness:
Staff should be aware of what constitutes an incident with particular emphasis on the less talked about situations such as harassment, GBV, near misses, or smaller incidents. Awareness can be raised while creating comfort and trust in encouraging incident reporting during induction, orientations, trainings, at meetings etc. Staff must know their rights and options.

Incident reporting options/procedures:
Several channels should be established for incident reporting. This offers additional options for personnel depending on their comfort level or need for confidentiality. Options include (but are not limited to): online reporting through agency intranet, phone hotline (reverse charges or toll-free), focal points, channels that bypass some levels of management (in cases where they are being reported on) etc.

Use of focal points:
Focal points must be carefully selected and trained based on their personal profile, capability, ability to maintain confidentiality and objectivity. Having a number of diverse focal points (international and national, male and female) can increase comfort and access to reporting.

Analysis/investigations:
Follow up on incidents will subsequently inform risk analysis, risk reduction measures or levels of staff awareness. Some level of internal investigation, conducted by extremely well trained individuals, may be necessary in the case of breach of internal policies. This will warrant notifying the local authorities /police for external investigation in case of a confirmed breach of local laws.

Disciplinary procedures:
Should there be misconduct by a staff member (depending on the severity of the incident, and local laws including labour laws) disciplinary measures should be taken and must be applied consistently across local/national/international/male/female staff members.

Institutional memory:
Avoid hiring any person with a history of perpetrating any type of serious incident including corruption, sexual harassment, or sexual violence, including sexual exploitation, sexual abuse and domestic violence. This may seem obvious, but there is a long history, through anecdotal evidence, of perpetrators being re-hired in a different country office – sometimes even by the same agency. If relevant

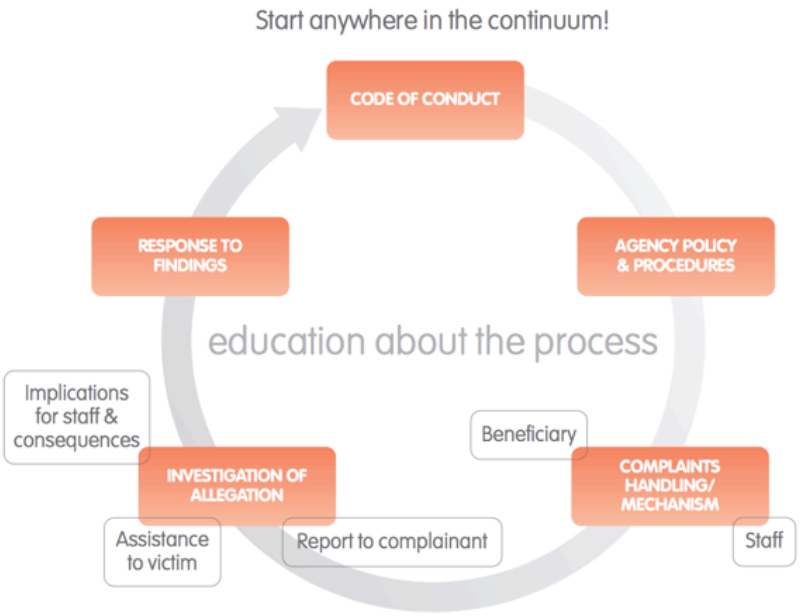
laws governing employers and employees permit, coordinate with other agencies to establish a system for sharing information about employees whose contracts have been terminated for engaging in harassment, sexual violence and/or SEA. Careful hiring practices that include reference checks and vetting are imperative.

Sexual exploitation and abuse (SEA) Framework

SEA Principles defined by the Inter-Agency Standing Committee (IASC)

- Sexual exploitation and abuse by humanitarian workers constitute acts of gross misconduct and are therefore grounds for termination of employment;
- Sexual activity with children (persons under the age of 18) is prohibited regardless of the age of majority or age of consent locally. Mistaken belief in the age of a child is not a defence;
- Exchange of money, employment, goods, or services for sex, including sexual favours or other forms of humiliating, degrading, or exploitative behaviour, is prohibited. This includes exchange of assistance that is due to beneficiaries;
- Sexual relationships between humanitarian workers and beneficiaries are strongly discouraged since they are based on inherently unequal power dynamics. Such relationships undermine the credibility and integrity of humanitarian aid work;
- Where a humanitarian worker develops concerns or suspicions regarding sexual abuse or exploitation by a fellow worker, whether in the same agency or not, s/he must report such concerns via established agency reporting mechanisms;
- Humanitarian workers are obliged to create and maintain an environment that prevents sexual exploitation and abuse and promotes the implementation of their code of conduct. Managers at all levels have particular responsibilities to support and develop systems that maintain this environment.

Reporting cycle SEA[40]



Source: InterAction SEA Learning Modules and Guidance

[40] InterAction. (2010). *InterAction Step by Step Guide to Addressing Sexual Exploitation and Abuse.* InterAction.

TOOL 8: ACTION PLAN FOR INCIDENT FOLLOW-UP

This tool lists questions to be included in a follow-up plan that should be implemented for every incident, despite its severity.

Incident reference number: #

Action to be taken (one line per action)	Description of the action to be taken in precise terms
By whom	At which level, name or position
With whom	Who is going to be involved, internally or externally to the organisation
Logistics required and budget	Estimated costs and needs, procurement procedures in the organisation
By when	By when is the action to be implemented? Fixed date or periodic review?
Who is responsible for the action being implemented	Is the manager responsible for it? The SFP? Anyone else?
Review and validation	By whom and which date
Signature	Signature of staff involved in implementation and control

Incident status:
Incident management status:

TOOL 9: SIIM SYSTEMS

Available systems to report, record, store and analysis security incidents that affected the organisation at a central level.

INCIDENT RECORDING AND REPORTING METHOD	SYSTEM	ADVANTAGES	DISADVANTAGES	FACTORS IN SET-UP AND RUNNING COST
Written narrative of the incident	• Emails • Google sheet • Shared Google platform • SharePoint	Very low set-up cost.	Only works well if used systematically. Risks: • Know-how and sometimes even access lost at times when staff leave. • Highly uneven reporting; with implications for the comparability of the information. Requires considerable time input during the analysis process.	Cost of staff time setting up the system. Cost of staff time writing the narrative reports. Cost of staff time turning the information into a systematic format. Cost of staff time carrying out the analysis, which is likely to be very time-consuming as the system itself does not support analysis.

INCIDENT RECORDING AND REPORTING METHOD	SYSTEM	ADVANTAGES	DISADVANTAGES	FACTORS IN SET-UP AND RUNNING COST
Excel spreadsheet to record incidents using systematic coding	Excel spread-sheet set up for the fields to be recorded. The Excel spreadsheet can be used to systematically classify information submitted in a written format.	Low set up costs. No consultant cost required as work can easily be done in-house. Can work very well for organisations that start out recording incidents and that have a limited number of incidents to record and manage.	Can become difficult to manage when too many categories and types of events are tracked. Requires a very manual trend analysis that can be time-consuming. Only the person with access to the spreadsheet tends to know and understand the system. Lower incentive for staff to report as they may remain unaware of the recording system.	Cost of staff time to develop an appropriate Excel system. Staff cost in translating written information into coded categories. Staff cost of carrying out the analysis.
Subscription to an online platform for data manage-ment	Some private companies and some non-profit organisations offer online platforms for security incident information management.	Efficient systems within in-built analysis functions. Most systems allow for different levels of access allowing tailored access for field staff as well as top management. Technical concerns are outsourced. Direct access for field staff increases the incentive to report. Ensures greater systematic provision of information as everyone uses the same system with the same instructions. Reduces workload for HQ analysis staff as analysis can be an in-built function.	Monthly running costs. Can be difficult or costly to request changes to adapt system to organisation-specific requirements.	Subscription fees.

INCIDENT RECORDING AND REPORTING METHOD	SYSTEM	ADVANTAGES	DISADVANTAGES	FACTORS IN SET-UP AND RUNNING COST
Custom-built online system	Some organisations have commissioned the development of organisation-specific online systems. Some organisations have been able to use existing systems and build the reporting as an extension to existing platforms used for email, such as SharePoint.	The system corresponds to organisational needs and internal definitions. If connected to existing systems, staff may learn how to use it much quicker.	High development costs if external IT specialists are needed. If organisations can use their IT department then costs are lower. Maintenance cost can be high if required to use external IT consultants but less if carried out by internal IT department.	Development and maintenance costs.

TOOL 10: INCIDENT STORING

Basic structures when using Excel spreadsheets to store incidents
Designing the ideal structure to store security incident information on an Excel spreadsheet is a very challenging task. The broad range of different events that should be considered for strategic decision-making around the security context and the detailed information required on some aspects make it impossible to have a simple structure that fits all situations. The challenge is to find the right balance between keeping it simple and workable yet storing the key information that is required, with enough detail to make the information meaningful for policy recommendations.

This guidance handbook provides two different format examples of how incident information can be stored on an Excel spreadsheet. Organisations designing their own spreadsheet are encouraged to look at both shared examples and mix and match the elements most suited to their own priorities. Please consult other tools for suggested definitions of the various fields.

The two example Excel spreadsheets for storing incidents can be accessed and downloaded from the RedR project page. Please on the below elements:

- SiND Event Categories spreadsheet
- Incident Log Template

Below are key principles to bear in mind when designing an Excel spreadsheet for security incident information.

Units of analysis
Each row on an Excel spreadsheet stores one key unit of information. In most cases, this will be the event. Each row is a unique event. The columns are used to provide details about the event.

To store other units of information, such as treating staff members as individual units (rather than a number associated with an event), or recording details on the material lost or tracking a response, can be done in the following ways:

- Create a second/third/fourth sheet on the Excel workbook for 'staff' or 'material' or 'response'. On these new spreadsheets, each row stores the individual information about each person, each item damaged or lost, or each response, etc. Each spreadsheet thus counts a different unit. If four

staff members would be affected in one event, the event spreadsheet would have one row (one unit) for the event but four rows (four units) on staff (see examples below). If two cars were damaged in the event, the 'material sheet' would have two rows, one for each car. Each staff member and car thus becomes a unit of its own. These sheets can be used to store details that are useful to have in the overall analysis.

  - The advantage of such a system is that that it becomes easier to provide detailed analysis beyond the event description. It is also possible to use dropdowns of multiple exclusive categories that are chosen for each individual. The sheet contains more information in a more condensed form. The disadvantage is that the data becomes more complex.
  - If additional spreadsheets are opened, it is vital to use unique event ID numbers in the first column to ensure it is possible to link the information back to the event.

- Integrate a different unit (such as staff, material) into the sheet where the unit of analysis is the event. This can be done by creating a series of additional columns each time the counting unit is changed from event to staff, material or response. Different colours can be used to indicate this.

  - For example, the columns could include the number of staff affected by the event by as many additional columns as are needed to classify all staff by additional information, which then needs to be split up into multiple options columns (see the Aid Worker Security Database spreadsheet as an example of how detailed information about staff can be recorded next to each other).

Some differences in information by single or multiple Excel sheets

The examples below show the same information about four people affected in a single event stored by unit of analysis 'event' and unit of analysis 'staff'. Storing the information on staff on a spreadsheet where the unit of analysis is the event requires more columns to store less detail. It is also not possible to store details about individuals (it would be very challenging to add the additional information on the job or whether the insurance covered the post-incident counselling). If staff are made the unit of analysis, it is easy to record more detailed information. This additional detail could help to spot trends or identify specific recommendations for action, for example related to insurance cover.

Single sheet for event units:

UNIT OF ANALYSIS	NUMBER OF STAFF AFFECTED	FEMALE	MALE	INTER-NATIONAL STAFF MEMBER	NATIONAL STAFF MEMBER	OTHER	DEATHS	INJURIES
Event 1	4	1	3	1	2	1	1	3

Multiple sheets for different units (e.g. staff, material or response):

UNIT OF ANALYSIS	UNIQUE EVENT ID	GENDER	STATUS	JOB	IMPACT	COUNSELLING INSURANCE COVER
Staff 1	Event 1	Female	International staff member	Professional staff	Injury	Covered
Staff 2	Event 1	Male	National staff member	Driver	Death	Not applicable
Staff 3	Event 1	Male	National staff member	Professional staff	Injury	Not covered
Staff 4	Event 1	Male	Volunteer	Volunteer	Injury	Not covered

Multiple or mutually-exclusive options
Information can be recorded as multiple options (more than one description applies) or as mutually-exclusive options (only one option can apply).

- **Multiple options** are presented in columns next to each other. Each column represents a particular characteristic and the spreadsheet is used to indicate that the specific option applies to the event. This can be done by choosing 'yes', a number (e.g. '1') or an option from a dropdown list. Options that do not apply are either left blank (less work in coding) or are identified as not applying by choosing 'not applicable' or '0' (this makes it easier to verify that total numbers are correct and to spot mistakes).
- **Mutually-exclusive** options are presented in the form of dropdown list options that can be chosen when filling in information in a particular column. Dropdown lists allow you to record additional information and ensure consistency in spelling. However, they should only be used if only one option can apply. See SiND Event Categories spreadsheet for dropdown examples.
- **Multiple and mutually-exclusive options** can be combined in data management. A well- designed spreadsheet can contain a series of columns presenting multiple options (e.g. all or some of the options may apply for each event and columns are filled in as required). These options have an associated list of mutually-exclusive dropdown list options (e.g. every time one of the options is chosen the system not only indicates 'yes' or a number but specifies the subcategory under the option). For an example of such a system see the SiND Event Categories spreadsheet.

TOOL 11: TECHNOLOGY TO REPORT AND RECORD INCIDENTS

Each system to report and record is different and has its own advantages and disadvantages. The model that is most appropriate to a potential organisation will depend on the level of technological capacity the agency has, the scale of its operations, size and financial resources, etc.

See the table below for a comparison of some online incident reporting systems.[41]

	FEE	OPEN SOURCE (FREE)	LICENSED	STAND-ALONE	SOFTWARE AS A SERVICE	STANDARD	TAILOR MADE	INTEGRATED GRAPHS	DATA PROTECTION LEVEL
Ushahidi		•		•		•			••
SIMSON	•		•		•	•		•	••
Open DataKit		•		•		•		•	••
SharePoint	•		•	•	•	•		•	••
NAVEX Global™	•		•		•		•	••	••
IRIS	•		•				•	•	••
RIMS			•				•	•	••

•• Not analysed

The following section presents the advantages and disadvantages of systems currently used by organisations that contributed to this handbook. To learn more about a system, please follow the links provided.

[41] Some of the information shared in this tool has been extracted from the forthcoming EISF article: De Palacios, G. (2017). *'Managing security-related information: a closer look at incident reporting systems'*, EISF.

SharePoint

This is a web-based application that integrates with Microsoft Office. It is primarily sold as a document management and storage system; however, the product is highly configurable and usage varies substantially between organisations. Although it requires buying a license for its use, some of the Microsoft Office 365 products are free for non-profit organisations. SharePoint is a system that can be used for sharing information in different forms; it is possible to create online forms that only authorised users can access.

ADVANTAGES	LIMITATIONS
As a Microsoft product, it is compatible with data processing software such as Word, Excel, PowerPoint, etc. This allows an organisation to easily export the data from the system to these applications and share and analyse the information using familiar software. It might not need new software installation or staff training on the use of the new platform. The development of the system can be managed internally by the IT team already in charge of developing and maintaining SharePoint.	Although it is possible to run surveys using SharePoint, it is not software specifically designed for reporting or collecting data. Representation of data in a map is not by default built into the system and it would have to be done through the installation of an additional complement.

Ushahidi

Ushahidi was developed to map reports of violence in Kenya during and after the post-election violence in 2008. Reports can be sent via a number of platforms including an online form, e-mail, text message or social media such as Twitter. Once these reports are received, they can be reviewed by an administrator in order to validate and approve the content, so that they can appear in the map of its main page.

Ushahidi is a free open-source software for information collection, visualisation and interactive mapping. The report form can be customised so that an organisation can collect the information that is important for it, and once reports have been validated it is possible to see them reflected in a map grouped per the pre-defined incident category. The platform can be programmed to alert security managers when a new incident has been reported, so that they can provide support to the victims and validate the report. Ushahidi can also alert other users once the report has been validated.

ADVANTAGES	LIMITATIONS
The main advantage with Ushahidi is that it can be downloaded from the internet for free. Installing the system is not complicated and since the organisation decides where to install the software, data remains under the control of the organisation.	The main disadvantage of Ushahidi is that statistical representation of the information contained in the database is not integrated into the system, and external solutions have to be combined for this purpose. It is an excellent solution for data collection, but other resources are needed for data analysis. The Ushahidi platform is no longer being developed, which could cause issues as other related technologies keep evolving. These potential issues can possibly be solved by IT staff.

SIMSON

The SIMSon system was specifically designed for NGOs by the Centre for Safety and Development (CSD). SIMSon is an online security incident reporting system where users can see the reported incidents represented on a map. NGOs that use SIMSon do not have to install, programme or write the code of any software. The Centre for Safety and Development (CSD) also provides support with running the platform and managing backups. Incidents can be filtered by categories, organisation, location, timeframe and other security-related information and indicators. Users receive e-mail alerts of new incident reports depending on their place in the organisation and their derived access rights. Incidents can be analysed within SIMSon by use of graphs and tables. Incident data can also be downloaded as an Excel file. Documents and incident reports can be uploaded, and at the discretion of the organisation, shared with other stakeholders, for example, insurance companies or other NGOs. There is a special 'sensitive incident' procedure that informs only designated officers in your organisation. This is relevant when dealing with for example sexual assault incidents.

To learn more, an overview of SIMSON can downloaded from the CSD's web page following this link.

ADVANTAGES	LIMITATIONS
The system is ready-to-use and is supported by the CSD. Organisations therefore do not have to invest resources in its development, maintenance, backups. Incident data can be analysed within SIMSon or by exporting the data to an Excel file.	Although the CSD guarantees organisations using the system that, if they choose, they are the only ones able to see their incident reports, NGOs may wish to control their security and incident related data and are reluctant to delegate this responsibility to third parties. Tailoring the reporting form for the specific needs of the organisation may not be easy.

World Vision International and NAVEX Global

World Vision International (WVI), in partnership with the international risk reporting provider NAVEX Global, have created an online incident reporting system for the communication of incidents, grievances, harassment and other events. This system goes beyond the strict communication of safety and security incidents and encompasses other elements of a risk management approach such as corruption, lawsuits, reputation, etc., in several languages. NAVEX Global adapts its reporting system to the needs and characteristics of the organisation using it. The incident reporting system allows input from a variety of sources and all WVI staff are able to report into the platform, since it also serves as a whistleblowing system.

To learn more about the World Vision International incident reporting system, see the following document.

ADVANTAGES	LIMITATIONS
The combination of incident reporting form with the whistleblowing channel, beneficiary complaint mechanism, etc. reduces the possible diversity of systems used for similar purposes. Having the support of a company dedicated to ethics and compliance management behind the system can help put incident reporting data in perspective with other risk management fields.	The form can be comparatively detailed which, despite its advantages, can discourage reporting due to its lengthy process. It is also probably a solution that only bigger organisations can afford.

IRIS

Based on Ushahidi, IRIS is a platform that can be used for reporting incidents through an online interface, and visualising where those incidents have taken place on a map. It is possible to customise the incident reporting template to accommodate the reporting needs of the organisation using the system.

The platform can be used as 'software as a service' as well as installing it in the servers of an organisation, allowing full control of the reported data. Only registered users can access the interface and different privileges can be set up depending on the user profile. Reports can be submitted through the online interface or through a low bandwidth connection.

The platform is multilingual and reports can be filtered by default or customised fields. Managers and other users can be alerted when new incidents have been reported so that immediate support can be provided to the victims while the rest of the team is informed to take appropriate actions.

Data can be extracted from the platform and fed to data visualisation software so that statistics about incidents can be used to draw lessons learned, give recommendations, provide briefings, use as risk analysis background information, etc.

ADVANTAGES	LIMITATIONS
Easy to install and use, highly customisable in its appearance and in the way the information is collected. IRIS is based on Ushahidi version 2, which being an open source platform, can be developed to accommodate the reporting needs of organisations using it, to adapt it to new developments and technologies and to make it compatible with other existing systems. Users are unlimited and it works without licenses, so organisations pay only for the installation and customisation. Existing data about incidents can be imported to the system upon installation.	The connection of the users list with the active directory of the organisation would have to be developed, but users can be created one by one and access to information granted during the process. The original software was conceived to widely share reported information. Although it is possible to have a 'reporter only' user profile, limiting access to information has to be carefully planned.

RIMS

The incident management service from the Risk Management Society (RIMS) offers a simple, easy to use system primarily using test-based incident descriptions. It allows for custom made categories to code aspects of the events. It is possible to set up graphs. The platform only exists in English.

In the example viewed, the system was mainly used by the HR department around insurances. The use of the system for security incident analysis was limited. It was therefore not possible to judge how well this system could have functioned if fully set up to serve needs for security incident information management beyond test-based incident descriptions, and in particular analysis.

ADVANTAGES	LIMITATIONS
Easy to use. Staff can use the system to report incidents without much training. It is easy to set up customised fields and to navigate the site. It is an easy and very accessible systems to store security incident descriptions.	The example reviewed used mainly text based event descriptions. The system does not send out reminders.

TOOL 12: ANALYSING AND COMPARING DATA TRENDS

Guidance when comparing organisation trend data with wider security incident data.

Key questions and considerations

- What are the similarities and differences in the trends between your organisation and those that appear within the pooled data?
- Why are there similarities and differences? Think about each observed aspect separately and ask:
  - Why do I see similarities or differences in this subcategory of incident types?
  - Is this because of the general external environment?
  - How are these trends affected by the countries your organisation works in or the programmes your organisation implements?
  - Could any of the differences be the result of reporting practices (yours or those of other organisations)?
  - Where does your organisation have more incidents of a particular type?
  - Where does your organisation have fewer incidents of a particular type?
- Look for similarities in the trends and try to give an explanation for similarities.
- Look at the differences. Try to suggest an explanation for the differences.
- Be sure you are accurate. If you know something to be a fact, state it. If you think but you do not have proof then use language that indicates this such as 'the data suggests', or 'it appears from the available information'.
- Identify key trends:
  - What key trends can be spotted?
  - Does the data suggest any emerging trends that organisations have to be mindful of?
- Describe the trends as specifically as is possible.
  - Are these global trends?
  - Are there trends in a specific country?
  - Which category of security events do they refer to?
  - Be as specific as possible by naming the incident types you see an increase in and where this may be happening. If you can, provide details of who or what may be particularly affected.

- Think about the overall trends of the general aid context as shown in the trend analysis or as visible within the data either at global or country level. Try to describe the overall context of aid delivery, recent changes and emerging threats or trends.
- Think about the differences in trends between the data of your organisation and that of other agencies (excluding any that are the result of reporting differences). Consider the countries your organisation works in, what programmes your organisations delivers, and weaknesses or strengths in your organisation's security risk management framework.
- If you are doing it for a second or third time, think about the differences between the most recent data and previous analyses. Describe changes and suggest explanations.
- Identify action to take:
  - Are there questions emerging from looking at the data that you could follow up on?
  - Who can help you to find out more?
- Contact the country/regional office/information service provider with questions to get an insight into the reality behind the data trends.
- Think about what to put on your action plan to implement over the next weeks/months.

Develop action plan

- Does the data suggest that the security focal point should take specific measures?
- Does the data suggest that new emerging risks or escalating situations should be added to the informed consent forms to discuss with staff?
- Does the data suggest that a particular event type should be given particular emphasis during training for a specific context?
- Does the data highlight specific risks that should be discussed in more detail with country and regional SFPs to see whether any changes in policy are needed?
- Does the data highlight issues that need to be brought to the attention to higher levels within the organisation?
- Does your analysis of the data suggest that your organisation needs improvements in security incident information management at some level within the organisation?

Possible issues to flag to colleagues whether in the field or at senior management/ Board level

- Name specific trends that ought to be closely watched. Suggest that they are put on a regular review agenda.
- Highlight a particular and specific risk and suggest an internal discussion on the acceptable risk threshold for a particular type of event in a particular context to help formulate a clear policy.
- Suggest specific activities for improved security incident information management to improve the organisation's ability to spot trends and request the go ahead to implement specific elements (see assessment grid for specific element that can be improved).

Communicate your final conclusions and action plan

Draft a concise and clear document that:

- Mentions the sources and methods used.
- Shows that you have considered the data and that you have confidence in your findings (you can include that you have dismissed looking further at a specific aspect because you think it is the result of reporting bias).
- Clearly list the trends that you think are a concern. Pick a maximum of three. If this is a regular exercise, include the key trends from the past analysis.
- List the action you recommend:
  - for yourself by specifying what you have been doing, are in the process of doing or you will be doing in the next months to address the identified needs:
  - for other colleagues (field or high level). Keep those for others to a single task by suggesting how you will be facilitating the process and what you will need from them as their input, support.

Compare your data with the data pooled by Insecurity Insight through the Aid in Danger Security in Numbers Database using either published trend analysis or by going to Humanitarian Data Exchange, in addition to your past security incident data.

See an example multi-agency trend data analysis report here.

TOOL 13: STRATEGIC-LEVEL QUESTIONS FOR INCIDENT INFORMATION MANAGEMENT-RELATED DECISIONS

Following a good overview of what kind of security incident occurred when, take a look at the data and think whether the data points towards a required follow-up action. Seek additional information and end the security incident report with specific recommendations.

The following list of questions can help security focal points when working out additional strategic-level conclusions and recommendations for actions following a good security incident analysis of past events.

QUESTIONS TO THINK ABOUT WHEN LOOKING AT THE ANALYSED SECURITY INCIDENT DATA	POSSIBLE FOLLOW-UP ACTION	POSSIBLE RECOMMENDATION FOR ACTION TO ADD AT THE END OF THE ANALYSIS REPORT
1. What kind of security incidents did staff and the organisation experience? **2. In which countries did they occur?**		
Does our organisation adequately prepare staff for the kind of possible events they may experience?	Find out to what extent people have been well prepared for the types of events that occur. Find out the cost of relevant courses and add a budget estimate.	Suggest the need for specific training or awareness courses for staff working in contexts affected by particular types of incidents.
Does the insurance cover required responses either for staff or to deal with material damage?	Find out from affected staff whether they received or would have liked to receive professional post incident counselling. Find out whether such counselling is covered by the insurance. Find out how easy or costly it was to replace lost items (insurance or other).	Suggest any gaps in the insurance cover. Suggest a strategy to deal with material loss for the country contexts where this appears to be a heightened risk.

QUESTIONS TO THINK ABOUT WHEN LOOKING AT THE ANALYSED SECURITY INCIDENT DATA	POSSIBLE FOLLOW-UP ACTION	POSSIBLE RECOMMENDATION FOR ACTION TO ADD AT THE END OF THE ANALYSIS REPORT
3. As security HQ focal point how satisfied are you with the way country offices appear to have used security incidents and near misses to learn and improve their practices? 4. What are the security incidents other organisations experience in the same country and how does this compare to the incidents reported within your organisation?		
Are there country offices that may not report systematically to HQ?	Seek a conversation with key personnel to find out why no or only a few incidents were reported.	Recommend the revision of instructions of how and when to report. Recommend changes the reporting system in a way that it encourages systematic reporting. Recommend better support from top management to signal the benefits of systematic reporting.
Are there country offices that experience particular types of incidents? How do these incidents compare to those experienced by other organisations?	Seek a conversation with key personnel to find out why particular incidents occur frequently or never.	
5. How did the security incidents affect the delivery of aid? 6. Can we cost the impact of security incidents on the delivery of aid?		
Have your colleagues reported the extent to which the incidents caused disruption to your work?	Seek conversations with colleagues on how best to describe the impact of security incidents on the delivery of aid.	Add statements on how security incidents affected the delivery of aid.
Have your colleagues costed the loss in staff time and material loss?	Seek conversations with staff of how best to cost the loss of staff time and material goods.	Add statements of the costs of security incidents to operations.
Have your colleagues reported the extent to which the security incident affected access?	Seek conversations with staff to describe how security affects access to beneficiary populations and how many people may not be reached due to security concerns.	Add statements of how security incidents affect access to beneficiary populations.
7. What were the main contexts of security incidents? 8. Can the context of incidents be classified by what response strategy may be needed?		
How many incidents may have happened because of failures in a good acceptance strategy? In which areas was there a failure of acceptance? Non-state actors, authorities, beneficiaries, staff, contractors or others?	Seek conversations within the organisation of the best acceptance strategy and how to implement it effectively.	Name the area or target population for whom a better acceptance strategy needs to be developed. Suggest improved training in acceptance strategy for staff going to a specific country on dealing with a specific actor.

QUESTIONS TO THINK ABOUT WHEN LOOKING AT THE ANALYSED SECURITY INCIDENT DATA	POSSIBLE FOLLOW-UP ACTION	POSSIBLE RECOMMENDATION FOR ACTION TO ADD AT THE END OF THE ANALYSIS REPORT
7. What were the main contexts of security incidents? 8. Can the context of incidents be classified by what response strategy may be needed?		
How many incidents may have happened because staff disrespected rules or regulations or behaved irresponsibly?	Seek conversations within the organisation of how best to promote ethical code of conducts for staff and ensure adherence to security procedures.	List behaviour aspects that might to be included into a code of conduct staff is required to adhere to. List areas of behaviour where staff disrespected rules and suggest mechanism for better enforcing them.
How many incidents may have happened because of personal factors related to the origin, background or family connections of the staff member?	Seek conversations within the organisation of how to address risk factors related to domestic life, ethnic origin or other private factors.	List contexts and countries where specific policies and procedures may be needed these could include: • How to respond if a staff member is affected by domestic violence • How to respond when there is a risk of ethnic discrimination or violence • What ethical code of conduct to expect from local staff where business interests or politics of extended family could affect staff.
How many incidents happened because the staff or the organisation happened to be in the wrong place at the wrong time?	Seek conversations within the organisation to what extent the organisation is prepared to accept general risks related to terrorism, crime or other incidents that do not target the organisation specifically.	List countries with heightened risk of incidents that are beyond the control of even the best security policies.
How many incidents happened due to action by state actors?	Identify the state actors responsible in internal documents and try to identify avenues to seek a dialogue with these state actors. Talk to advocacy colleagues and consider developing a joined campaign with other NGOs to raise awareness.	Suggest possible avenues for conversations to be followed up by country representatives or senior management using diplomatic channels or the support from other agencies (e.g. ICRC). Identify areas where an organisation could consider an advocacy campaign with others, such as the bombing of infrastructure or impunity from prosecution.

QUESTIONS TO THINK ABOUT WHEN LOOKING AT THE ANALYSED SECURITY INCIDENT DATA	POSSIBLE FOLLOW-UP ACTION	POSSIBLE RECOMMENDATION FOR ACTION TO ADD AT THE END OF THE ANALYSIS REPORT
9. Can we use the data to identify a risk threshold our organisation is prepared to accept		
What kind of decisions were taken throughout the period under analysis that give an indication of the risk threshold the organisation is prepared to take?	Think critically about your own decision-making in relation to security risks. What are the principles and thresholds you base this on? Seek conversations with other staff in the organisation and consider whether you use the same principles and thresholds.	Recommend the development of a clearly articulated threshold of risk to be communicated to staff.
How consistent was such decision-making between different contexts?		
Does there appear to be relationship between the security incidents reported and the specific decisions taken?		