SECURITY INCIDENT INFORMATION MANAGEMENT HANDBOOK

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

Publication date: September 2017

'Security incident information management involves collecting, recording, analysing and using information to maintain staff security and access to beneficiaries.

Good security information management finds the right balance between these benefits and the administrative costs of the system.'

ACKNOWLEDGMENTS

This handbook was developed collaboratively between RedR UK, Insecurity Insight and EISF, as part of the Security Incident Information Management (SIIM) project, funded by EU Humanitarian Aid. For more information please consult RedR's project page.

The project coordinator was Marine Menier (RedR UK). This handbook received significant input from Christina Wille (Insecurity Insight) and Lisa Reilly (EISF). The editor was Adelicia Fairbanks (EISF). The project team would like to thank the Advisory Group members and other contributors – too many to mention individually – for sharing their expertise, tools and very useful remarks with us. The SIIM Project acknowledges the breadth of contributions made and willingness of organisations and individuals to be involved.

DISCLAIMER

This handbook is one element of a broader project aimed at building the capacity of the humanitarian and development sectors; other capacity building activities are complementary to this tool. This document reflects current practices in the sector, provides recommendations and observations, including views or recommendations of third parties. It is not prescriptive, and is a work in progress.

While the SIIM Project has endeavoured to ensure the accuracy and quality of the information presented in the Security Incident Information Management Handbook, RedR UK, Insecurity Insight and EISF will not be liable to the fullest extent permitted by law for any loss, damage, or inconvenience arising as a consequence of any use of or inability to use, or interpretation of, any information contained within this handbook. RedR UK, Insecurity Insight and EISF will not assume responsibility and will not be liable to you, or anyone else, for damages whatsoever incurred for any decisions made or action taken in reliance on the provided information in this Security Incident Information Management Handbook.

The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained within this document shall be entirely at your own risk.

Designed by Tutaev Design

ABBREVIATIONS

AiD	Aid in Danger
AWSD	Aid Worker Security Database
EISF	European Interagency Security Forum
FAQ	Frequently Asked Questions
HQ	Headquarters
IASC	Inter-Agency Standing Committee
ICRC	International Committee of the Red Cross
IGO	International Governmental Organisation
IHL	International Humanitarian Law
INGO	International Non-Governmental Organisation
ISO	International Organization for Standardization
LNGO	Local Non-Governmental Organisation
NGO	Non-Governmental Organisation
PFA	Psychological First Aid
SEA	Sexual Exploitation and Abuse
SFP	Security Focal Point
SIIM	Security Incident Information Management
SLT	Saving Lives Together
SOPs	Standard Operating Procedures
UNDSS	United Nations Department of Safety and Security
WHO	World Health Organisation

CONTENTS

INTRODUCTION

About this handbook

Security incident information management (SIIM) is the collection, reporting, recording, analysis, sharing and use of information (including data) linked to a security incident. Security incident information management is a key part of an organisation's broader security risk management, which aims to support organisational security in order to ultimately improve access to populations in need.

The SIIM Handbook seeks to make an important contribution in advancing practices related to security incident information management within non-governmental organisations (NGOs).

The handbook is intended to support users in establishing and developing effective information management for security event reporting and monitoring systems, both internally and externally, across the organisation and the sector.

This document is part of a broader SIIM project, which is aimed at strengthening humanitarian responses to crises by building the capacity of NGOs to improve security incident-related information management, and enhancing their ability to share incident information in a safe and appropriate manner to support good decision-making across various levels of an organisation.

The *SIIM Handbook* presents a broad range of tools and guidance, from advice on how to design an effective security incident report to sharing security incident information efficiently with a wide range of relevant stakeholders. The security risk management approach and vocabulary presented in these guidelines follows the global standard issued by the International Organization for Standardization (ISO), 'Risk management – principles and guidelines' (henceforth ISO 31000:2009).

This handbook deals with security incident information management, not with the management of security incidents as such.

Most of this handbook is applicable to all types of incidents, including critical incidents, that is, events that disrupt normal, routine operations and require an organisation's crisis management response. Throughout, the term 'incident' will be used to refer to all types of incidents. When referring to a critical incident, this will be specified. Reference may occasionally be made to 'non-critical incidents', which will refer to all incidents that would not be considered critical and therefore not require a crisis management response. It is important to stress, however, that while some incidents may be deemed critical by one organisation, they may not be deemed so by another organisation that has the capability to deal with the incident through routine management procedures.

Although often undervalued, collecting and managing information related to incidents that are not deemed critical, including 'near misses', can be as important for analysis

and sound security-related decision-making as information from critical events. This handbook, therefore, provides tools to help develop standards for the reporting and information management of all incidents, including those that occur more commonly and would generally not be deemed critical.

This handbook reflects current practices in the sector, and provides recommendations and observations for NGOs. It draws on resources from a broad range of experts including the European Interagency Security Forum (EISF), Insecurity Insight, RedR UK and many of their member organisations and broader networks. While using existing tools and guidance, it aims to avoid duplication by highlighting and drawing out the elements of security incident information management. This handbook is not prescriptive, but rather offers a wide menu of options for organisations to strengthen their security incident information management.

Although this handbook was written with a focus on humanitarian organisations and operations, the information is broadly applicable to other NGOs as well, particularly development-focused organisations.

This version of the handbook (published September 2017) incorporates feedback and input received from stakeholders within the humanitarian and development sector.

This is an open-source document, and will be made available online in English, French and Arabic.

Who is this handbook for?

The *SIIM Handbook* is intended for all individuals with any level of responsibility for security incident information management within a non-governmental organisation, irrespective of their position or location. It is designed as a tool for security advisors, managers, focal points and analysts, as well as senior management and general project/programme managers who have a security responsibility within NGOs, and is primarily for practitioners.

How to use this handbook

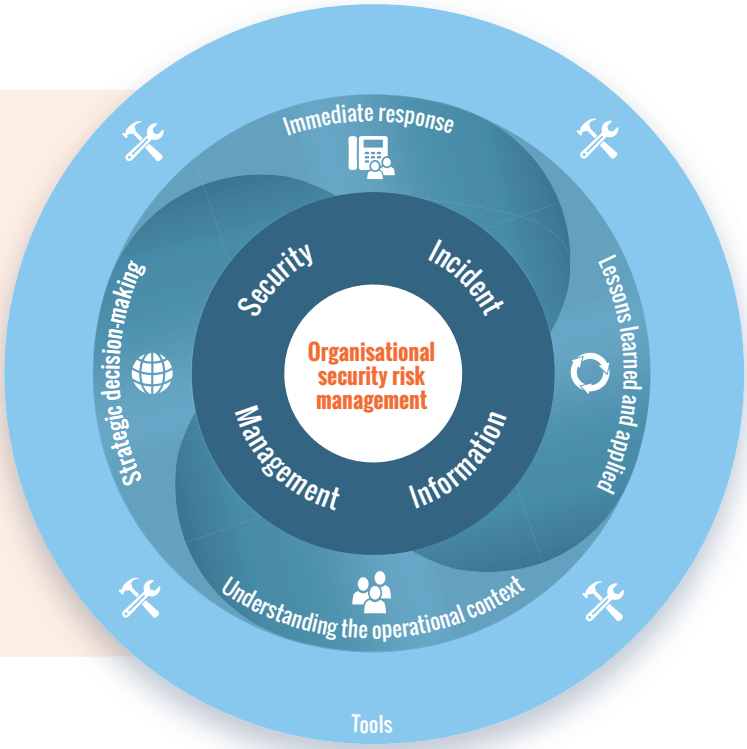
The *SIIM Handbook* is divided into chapters, providing an overview of security incident information management:

- The handbook initially introduces the concept of SIIM and how it fits into the broader security risk management of an organisation.
- It goes on to present four key objectives of SIIM, highlighting key steps involved in the effective management of security incident information to achieve each objective.
- Tools are referenced throughout the text and can be found at the end of this handbook.

The following diagram illustrates the different components of security incident information management. The structure of this handbook follows this diagram and each section of the handbook will indicate which part of the cycle is being discussed.

SIIM Cycle: Organisational security to obtain unhindered access for the delivery of aid

The diagram is cyclical to show that security incident information management is an on-going process in which all elements feed into each other to meet four primary goals. At the heart of security incident information is organisational security with the objective of unhindered access for the delivery of aid.



This handbook provides discussion points, tips, advice and suggested templates, across four primary objectives of security incident information management that relate to four distinct timeframes and different levels of organisational focus:

Objective one: to inform immediate reaction and response to a security incident. The purpose is to ensure that information is sought and used to inform the immediate response to the incident. This usually occurs at field and/or country level soon after the incident has taken place.

Objective two: to implement lessons learned after a security incident for follow-up action and prevention. The purpose is to understand what happened with a view to planning and implementing any necessary changes and procedures that will help to treat the risk of similar future events, with a particular focus on prevention. This usually occurs at country/headquarters (HQ) level shortly after the security event.

Objective three: to understand the NGO security context. The purpose is to improve contextual knowledge by using internal and external incident data. This will help inform strategic decisions, global communication and self-reflection among aid agencies. This usually occurs at country level and at a senior management level within HQ, and is best reviewed on a regular basis.

Objective four: to inform strategic decision-making in an organisation. The purpose is to take stock of the changing nature of incidents, to understand the most challenging working environments, the organisation's overall exposure to risk, and to identify the best strategic responses. This occurs at country, regional and HQ level within a reasonable amount of time after a security event and during planning and programming phases.

It is important to consider the four objectives as part of a whole, all of them feeding into the overarching objective of reducing security risk for the organisation, thereby improving aid access to populations in need.

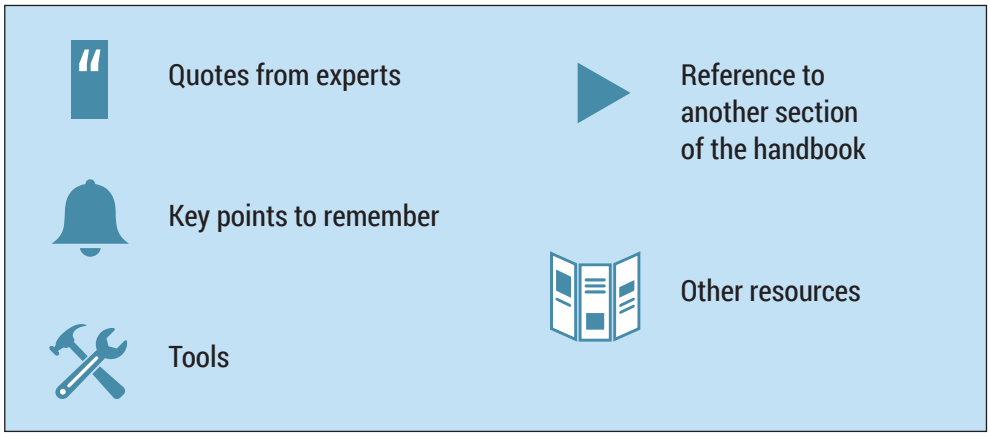
Each section provides guidance on key steps and how to create standards and well-defined categorisations that enable organisations to analyse data more easily. When data is shared between agencies, standard definitions and ethical procedures are essential.

Organisations and their staff are invited to:

- Use the handbook to obtain a stronger understanding of security incident information management and what key steps can be followed to improve their organisation's overall security risk management.
- Use the tools provided at the end of this handbook to improve their organisation's security incident information management system. Find a list of the tools here.
- Use the 'Tool 1 : SIIM self-assessment grid' to assess the security incident information management needs of their organisation. This review should be done at regular intervals. After a defined period of time, organisations should reflect on their progress since their initial self-assessment.

The handbook can be consulted as a whole or individual chapters, or tools, can be given to specific staff. The four primary objectives outlined in this handbook are distinct but interconnected: improving practices to meet one objective will help an organisation meet the other objectives, and as a whole contribute to operational preparedness and organisational security.

For ease, the following icons are used throughout to guide the user in identifying the types of resources provided:



For easy navigation, tools and references to external resources, as well as cross-references to other sections within the handbook, are hyperlinked.

Boxes on the right side of each page are hyperlinked to the start of the identified chapter. By clicking on this tab on the first page of a chapter, the reader is sent back to the table of contents.

References in the footnotes are hyperlinked to the 'References and Bibliography' at the end of the handbook.

Key definitions

Analysis: the process of turning unorganised facts, figures, objects, etc., into meaningful information which can be used for different purposes, such as informing decision-making.

Analytical skills: the ability to visualise, articulate, conceptualise or solve both complex and uncomplicated problems, including the ability to apply logical thinking to break complex problems into their component parts.

Crisis: an event that requires a response greater than that possible through routine management or procedures. The response may require additional input from specialist and/or higher-level management (likely at headquarters level). Many organisations will categorise as 'critical' an incident that must be managed as a crisis situation.

Data: facts and statistics collected together for reference or analysis; information in a raw or unorganised form that refers to, or is represented by, conditions, ideas, or objects.

Duty of care: 'the responsibility or the legal obligation of a person or organisation to avoid acts or omissions, which can be reasonably foreseen, to be likely to cause harm to others'.[1] Organisations should also consider their moral duty of care.[2]

Event: an occurrence or change of a particular set of circumstances. Within this handbook, an 'event' is used interchangeably with 'incident'.

Horizontal information flow: the sharing of information laterally between organisations, and between organisations and stakeholders.

Incident: any event(s) in which staff safety or security is compromised; any dependant or other third party is injured or harmed in the course of the organisation's activities; property or belongings of the organisation are stolen, damaged or put at risk; where there is interference with the delivery of aid and/or the independent work of the aid agency is compromised, including reputational damage.

> **NOTE:** Incidents can be organisational (affecting the organisation directly and its ability to deliver aid) as well as external (affecting others outside of the organisation). Reporting both can be beneficial to security incident information management.

Incidents can further be categorised as:

Critical incident: an incident that disrupts normal, routine operations. A critical incident can result in death, life-threatening injury or illness and triggers an organisation's crisis management response. These incidents tend to require an urgent response.

Near misses: events that almost result in harm, damage or loss to the organisation, its staff or programmes or had the potential to result in serious injury, death or kidnapping and only caused minor injury, damage or loss. Can also be referred to as a 'near hit' or 'close call'.

1 Kemp, E. and Merkelbach, M. (2011). 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff', *Security Management Initiative*.

2 Kemp, E. & Merkelbach, M. (2016). *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF)

NOTE: Administrative impediments (e.g. overly bureaucratic customs and excise barriers, granting of visas or travel permits to disaster-affected areas, etc.) may be considered and reported as incidents, as they can also provide information on the context.

Accidents: random events that result in harm, damage or loss to an organisation, its staff or programmes. In contrast, 'incidents' are motivated by the will of individual(s) to cause harm to persons or entities, to seize assets or to disrupt the delivery of aid, either by direct targeting of that agency or agency personnel, or otherwise. No matter whether an event is a security incident or an accident, both should be reported. However, when this handbook refers to 'incidents' or 'security incidents' it is referring primarily to security- related events. Nonetheless, the reader is asked to keep in mind that the models, tools and guidance contained herein also provide useful guidance in managing information related to accidents, such as road traffic accidents.

Information: what is conveyed or represented by a particular arrangement or sequence of data. It is the communication or reception of knowledge or intelligence. Raw data is transformed into information by analysis.

Information management: the umbrella term used to describe policies and guidelines designed to:

- regulate the types of information organisations collect, store and communicate;
- reduce the risks to staff and organisations inherent in these processes; and
- ensure that information can be accessed by the right people in a timely manner.[3]

Information owner: the individual (or group of individuals) with the ability to create, edit, modify, share and restrict access to the data.

Information security: the 'preservation of confidentiality, integrity and availability of information…Other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved'.[4]

Personnel: staff, volunteers, and any other individual coming under the organisation's umbrella, including consultants, partners, visitors, etc.

Risk: 'the effect of uncertainty on objectives'.[5] A risk can also be the likelihood of a threat affecting the organisation and the impact it will have if it does.

Risk assessment: a process to identify security and safety threats that could affect staff, assets and programmes, and analyse their likelihood and impact, in order to determine the degree of risk involved.

Safety: freedom from risk or harm resulting from unintentional or accidental acts, events or hazards.

3 Ayre, R. (2010). *The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field*. EISF.
4 ISO/IEC 27000:2014
5 ISO 31000:2009

Security: freedom from risk or harm resulting from intentional acts of violence, aggression and/or criminal acts against agency staff, assets or property.

Security incident information: data and information linked to a specific security event or a sequence of events.

Security incident information management: the collection, reporting, recording, analysis, sharing and use of information (including data) linked to a security incident with the overarching aim of obtaining unhindered access for the delivery of aid by improving organisational security risk management.

Security risk management framework: a set of policies, protocols, plans, mechanisms and responsibilities that supports the reduction of security risks to staff, programmes and an organisation.

Sexual violence: 'any sexual act, attempt to obtain a sexual act, unwanted sexual comments or advances, or acts to traffic a person's sexuality, using coercion, threats of harm or physical force, by any person regardless of relationship to the victim, in any setting, including but not limited to home and work. Sexual violence takes many forms, including rape, sexual slavery and/or trafficking, forced pregnancy, sexual harassment, sexual exploitation and/or abuse, and forced abortion.'[6]

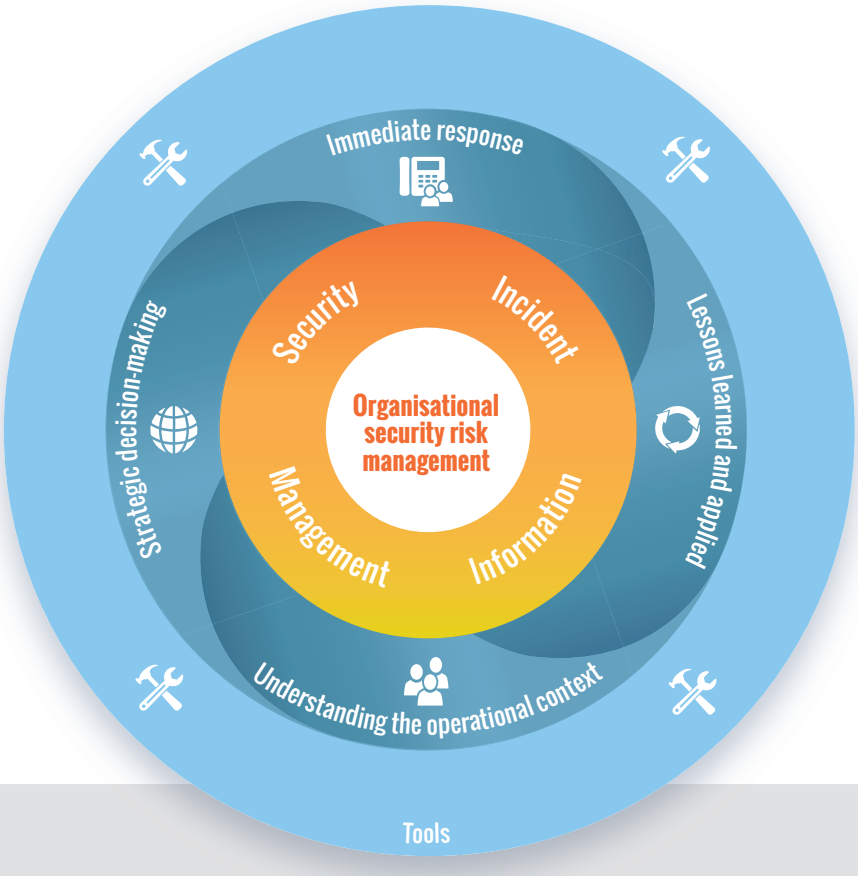
Typology of incidents: the classification of incidents according to general types.

Tool 2: Typology of incidents proposes a typology that is used by Insecurity Insight in its analysis and is based on typologies of several organisations.

Vertical information flow: information travelling up and down within an organisation's structure. When a stakeholder in a region collects incident reports and sends them to headquarters for more detailed analysis, it is an ascending information flow. As information is analysed and conclusions are drawn, they may be disseminated in a descending direction to field staff.

[6] Inter-Agency Standing Committee (IASC). (2015). *Guidelines for Integrating Gender-Based Violence Interventions in Humanitarian Action: Reducing risk, promoting resilience and aiding recovery.*

CHAPTER 1: INTRODUCING SIIM



This section introduces security incident information management and discusses how it fits within a broader security risk management approach, in order to reinforce prevention of, and preparedness for, security incidents.

- What is security incident information management?
- Key challenges in security incident information management
- Security risk management and SIIM
- Staff security competencies and SIIM
- Information security
- Incident management and SIIM: the benefits of organisational preparedness
- Duty of care

Relevant tool:

- Tool 1: SIIM self-assessment grid

What is security incident information management?

Security incident information management is the collection, reporting, recording, analysis, sharing and use of information (including data) linked to a security event or sequence of events.

Effective management of security incident information enhances a NGO's ability to share and use incident information internally and externally in a safe and appropriate manner to support good decision-making across various levels of an organisation.

Security incident information management should not be limited to severe events of death, injury or kidnapping nor to the most affected countries. It is beneficial if all incidents affecting the delivery of aid are reported and analysed by organisations. This enables organisations to (among other things):

- Adopt appropriate and effective risk reduction measures immediately, allowing managers to be informed quickly so they can offer the necessary support to staff affected or involved in an incident;
- Improve context analysis by establishing trends and emerging patterns on the basis of which informed operational decisions can be made by senior managers;
- Inform external stakeholders of potential threats and risks so they too can put in place risk treatment measures;
- Maintain a full institutional record of security incidents.

The key steps in security incident information management are:

- Reporting.
- Recording.
- Analysing data collected through an incident.
- Information sharing (internally and externally).
- Decision-making at field level, usually as an immediate response to an incident.
- Decision-making at country or regional level, using information on incidents reported to apply lessons learned to improve security procedures.
- Data analysis of incidents to identify trends and patterns.
- Using trend analysis to inform contextual analyses, risk assessments and make informed decisions on the best risk treatment measures to put in place to improve organisational security.
- Strategic decision-making at headquarters level that involves the use of trend analyses established from incidents reported to make informed organisation-wide decisions.

These key steps will be discussed in more depth in 'Chapter 2: The four objectives of security incident information management'.

Key challenges in security incident information management

Challenges to security incident information management can be linked to both individual and organisational factors.

Under-reporting
Many incidents are never reported or recorded. Non-critical incidents are more often reported than near misses although both are under-reported. This does not mean that these types of incidents do not happen, just that they garner less attention in comparison to other incidents that carry far greater risk in more hostile environments.

Non-critical incidents in hostile environments can be indicative of a deterioration in the situation and worsening tensions and should be reported to the appropriate line manager or security focal point (SFP) and may suggest a need to review the context and risk analysis of the organisation.

Differences in definitions
Perceptions as to what constitutes an incident can vary greatly between organisations, as well as between individuals within the same organisation. One NGO may feel that a short burst of gunfire during the night is worth reporting, whilst another may not if the operational environment is such that gunfire is a common occurrence. Similarly, international and national staff may have different perspectives about what represents an incident that needs reporting.

Managers need to give clear guidance on what constitutes an incident that requires reporting in given locations, to ensure a consistent approach throughout the organisation.

All personnel should have a common understanding of the terminology associated with security incident information management so they can communicate effectively – both internally and externally. A lack of consistency in the use of terms is problematic for analysis. For example, security documents may mention related or similar incidents such as 'robbery' and 'theft' without defining the distinction.. In order to pool and compare data from different agencies, as well as across different countries within an organisation, it is necessary to have common definitions.

Reputational concerns
A security incident indicates that something somewhere has gone wrong. Even though aid organisations are rarely responsible for a security incident occurring, they can often identify elements related to their procedures or staff behaviour that in some form may have either contributed to making the event possible or affected the consequences of the incident. Due to the potential impact information related to incidents might have on an organisation's reputation, many NGOs may prefer not to share details of what went wrong, particularly with external actors.

"Learning from near misses as well as mistakes is standard practice in other industries. In the aviation industry, for example, all companies are obliged to report any failure – whether technical or human – and this has been used to develop guidance that has made flying one of the safest means of transport today.[7] Therefore, sharing the learning from what has gone wrong within one NGO could help the humanitarian and development community as a whole."

Organisations benefit from clearly outlining at a policy level when to share incident reporting information internally and externally, how to ensure confidentiality when required, and what steps to follow in order to judiciously manage the information.

Administrative burden

Documenting incidents is time-consuming and absorbs important human resources. If organisations manage to put an efficient system in place, however, the administrative burden can be lessened, thereby avoiding staff having to spend time searching for the instructions on how to record and report incidents. Providing tools and templates helps to make recording and reporting not only more consistent throughout the agency but also less laborious and therefore more likely to happen..

The incident information management policy and procedures should be explained to staff and kept as simple as possible.

Organisational culture

Managers, at any level, have a responsibility for sharing information vertically within the organisation, e.g. to their line manager or headquarters, but appropriate information is often not shared for a variety of reasons. Managers (national and international) may not share information vertically for fear of administrative backlash, admission of breaking a policy, or to 'save face'. National staff members who are on the frontline bear the brunt of NGO deaths and injuries, but may feel that if they report an incident their reputation may be affected. Many fear that they may be penalised through fewer opportunities for promotion or, in the worst-case scenario, lose their job.

Any misbehaviour or breach of security procedures (or code of conduct) can be revealed by the analysis of incidents. The organisation can decide if disciplinary measures are needed. This question is often subject to debates within organisations, who consider the question of sanctions as an additional factor for non-reporting. Organisations would benefit from having a clear stance on this and balancing these concerns.

Response to breaches in security procedures must be consistent. Security policies are ineffective if senior management or security staff break them without consequence.

Communication between agencies

Sharing security information, including incident and situation reporting between organisations, can be difficult. Overcoming the primary challenges to collaboration, such as confidentiality, trust and management of information, are discussed in more depth in 'Objective three: Understanding the operational context'.

7 Wille, C. (2016). 'Lessons from the Aviation Industry: What Can We Learn for Humanitarian Security Risk Management?', *EISF*.

Security risk management and SIIM

Security risk management involves an organisation putting in place policies, protocols, plans, mechanisms and delineating staff responsibilities to support better access through improved organisational security. The below diagram, which illustrates an organisation-wide security risk management framework, presents the different pillars that enable effective security risk management.[8]

While incident monitoring is highlighted as a core pillar of the SRM framework, well-managed security incident information can feed into and strengthen all key elements of security risk management.

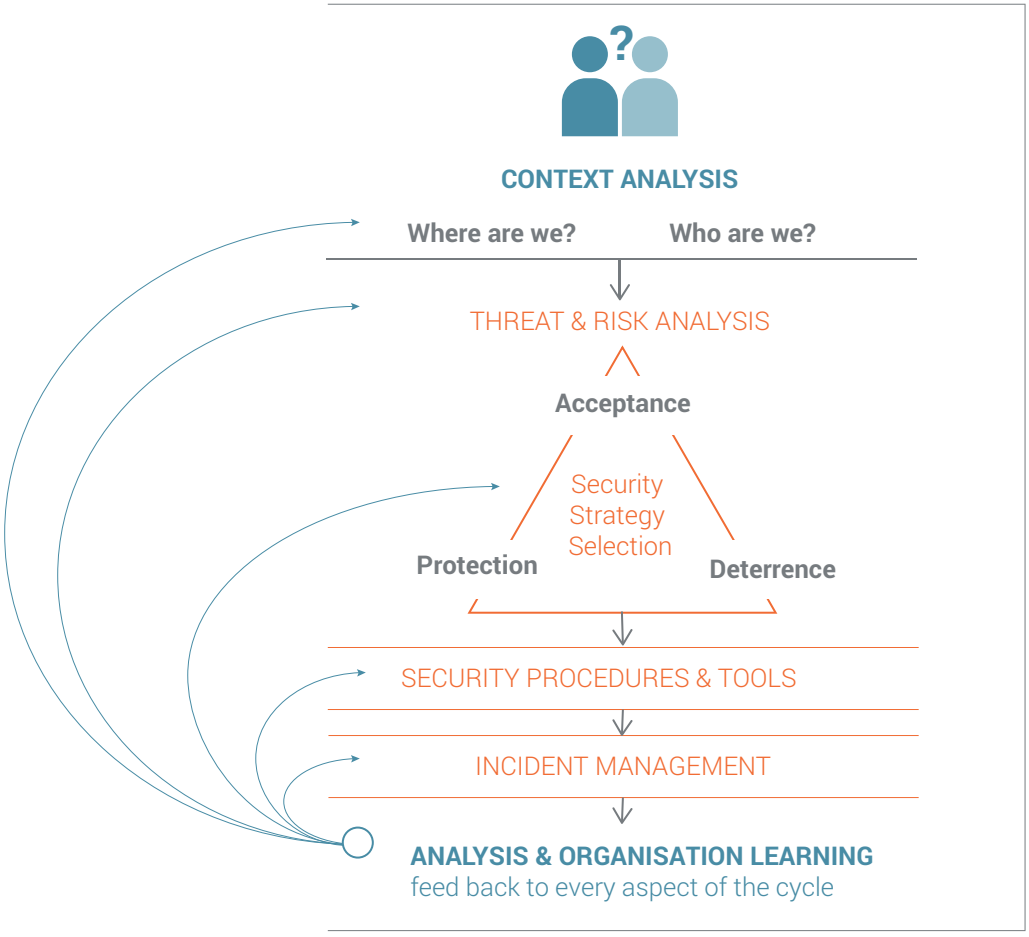
From ensuring that crisis management structures are set up in a timely manner after a critical incident to using non-critical incident information to inform staff of travel risks, security incident information management is a crucial element of good security risk management.

> *"An incident is the perfect occasion and opportunity to learn and improve. Its analysis should feed into the entire security management framework."*

Security focal points and security analysts can use information from internal incidents and other sources to understand the context in different locations. Information extracted and analysed after an incident should inform the organisation's risk analysis by highlighting threats and vulnerabilities in the given context. It can inform the review of standard operating procedures (SOPs) and contingency plans, and can also be used as good supporting evidence to institute policy changes.

[8] Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs.* EISF.

The following diagram[9] illustrates key steps in security risk management. Good management of incident information will enable organisations to use this information to inform each step in this process.



Staff security competencies and SIIM

The body for NGO security professionals, INSSA (International NGO Safety and Security Association), includes information management as one of their key competency areas for country, regional, global and strategic security responsible staff.

Staff at each level will support the organisation's overall security risk management systems and procedures, and it is extremely important to:

- Clearly delineate the security responsibilities for staff at each level; and
- Ensure that staff have the sufficient support and training to meet their responsibilities in line with the level at which they find themselves.

See the 'People management module' within EISF's guide 'Security to Go' for more information on the interconnection between people management and organisational security.

[9] This diagram comes from RedR UK's introductory security courses.

Information security

In the context of security incident information management, it is important for an organisation to ensure the means of communication used for reporting, collection, analysis, sharing, storing and use of information are secure.

Organisations often have to balance the need for safe security incident information management and budgeting constraints. It is nonetheless crucial to address data security, whatever the available financial resources. For an analysis of radios, mobile phones, satellites, emails and other technical aspects of information management, please refer to ODI's GPR8 guide for a chapter on telecommunications and EISF's 'Security to Go' guide.

The legal and ethical duty of NGOs to ensure the confidentiality of information is paramount, particularly if it is 'personal data' – i.e. any information relating to an identified or identifiable person. Failures in creating or implementing information management policies can have negative repercussions for staff and organisations, and could result in legal action and redress.

"Good security incident information management is in part about achieving the correct context-determined equilibrium between the benefits that collecting, recording and communicating certain sets of information bring, and the risks these actions entail."

NGOs should strengthen their information management culture by ensuring information security is embedded in wider risk management policies and procedures, and seamlessly incorporated into organisational and programmatic thinking. Most risks can be mitigated through risk awareness, common sense and good discipline: referred to here as 'good housekeeping'. Good housekeeping covers paperwork and hard copies as well IT security – the best IT security in the world will not protect from staff leaving documents on their desk at night or putting sensitive documents in the bins without shredding them.

Information security is not a challenge to be addressed by IT departments alone. 'Good housekeeping' and technical solutions are underpinned by effective staff training and sufficient resources, constituting a strong information management culture in which staff implement security policies almost automatically.

To ensure good information security in security incident information management, organisations should address the following key issues at all levels and all stages of collection, reporting, recording, analysis, use and sharing of information:

- **Physical security:** the protection of computer hardware, office facilities and organisation assets from physical circumstances and events that could cause serious damage or loss, including theft, fire, and natural disasters.
- **Digital security:** the protection of electronic files stored on computer devices – from mobile phones and PDAs to USBs and computers – from unauthorised access, corruption, loss, misuse or destruction. Basic digital security measures should always be observed, such as password-protecting user accounts, wireless internet networks, and sensitive documents.
- **Accessibility:** the categorisation of information and staff so that information is only accessible to staff in relevant roles or of sufficient seniority (see 'Categories of information' in 'Objective three').

- **Back-ups:** guidelines on how, and how frequently, to back up files, ensuring that programme interruption is kept to a minimum, since the risk of hardware damage or loss can never be completely eliminated.
- **Destroying information:** clear guidelines on how and when information (in both hard and soft form) is to be destroyed, with an awareness that this may have to be done quickly. In high-threat environments, especially those in which sophisticated surveillance is suspected, certain types of information should perhaps not be collected and recorded at all. Additionally, sensitive information management should be clearly separated from routine information management. Thus, should a deteriorating context mandate a rapid destruction of sensitive information, it will be possible to rapidly identify what needs destroying.
- **Communications security:** an information management policy should identify how and what to communicate in particular environments. Information is perhaps most vulnerable when being communicated: radio is not secure, telephone calls can be bugged, emails intercepted, etc...

See ODI's GPR8 guide for a chapter on communications security.

Security-in-a-box

A key component of information security is strong digital security tools and tactics. 'Security-in-a-box' is an initiative jointly developed by Front Line Defenders and Tactical Technology Collective, that resulted in the development of community guides providing tailored advice on tools and tactics that are relevant to the needs of particular groups of individuals. These cover the basic principles of social networking platforms and mobile phones, including advice on how to use these more securely. Security-in-a-box's tools and tactical guides offer step-by-step instructions on how to install and use the most essential digital security software and services (these resources are available to download from their website).

Incident management and SIIM: the benefits of organisational preparedness

Although the management of incidents is not the focus of this handbook, we suggest that security incident information management is a key component of incident management and organisational preparedness.

Organisational preparedness means having in place clear procedures and training on incident management and incident information management, which will ensure the best possible reactions and responses to events.

Incidents, particularly critical ones, usually have the following characteristics:

- an element of surprise;
- insufficient information;
- escalating events that may outpace response;
- important issues resulting in outside scrutiny;
- loss of control (real or perceived);
- disruption to normal decision-making processes; and
- those directly affected tend to adopt a short-term focus.

Unless incidents are critical, they are usually dealt with within the framework of pre-established procedures. Even non-critical incidents, however, can create confusion and panic for those who are not prepared to respond to them.

The purpose of security incident preparedness and management is to reduce the impact of incidents and to enhance an organisation's ability to cope with the present and learn for the future.

Following an incident, an organisation will aim to:

- prevent further harm and ensure the health and/or safety of victim(s) and staff;
- assure staff and the families of victims that a responsible and effective response is underway;
- ensure continuous organisational management throughout the incident, particularly if it is an ongoing event, such as a kidnapping;
- ensure programme continuity;
- reduce loss of assets (such as phones, computers, vehicles, etc.);
- replace assets lost through robbery, etc.
- fulfil organisational responsibilities and reduce the risk of litigation/liability claims;
- file complaints (for example, notifying competent local authorities of any threats against staff);
- safeguard the organisation's image and reputation;
- share critical information with other NGOs and partners who may also be at risk during or after an incident;
- prepare press releases and/or inform media and outlets of humanitarian/development news with selected information that informs the public while protecting those involved.

Security awareness, threat, vulnerability and risk analysis, effective procedures, the holding of security and safety drills, extensive networking with partners and external agencies and good contingency planning are all proactive ways of dealing with incidents and therefore potential crises.

Organisational preparedness is key for effective incident management and security incident information management.

Although policies cannot cover every eventuality, having contingency plans and incident management plans, regularly updating them to work through 'what if?' scenarios, as well as having effective crisis management procedures in place, will go a long way towards keeping a situation under control and maintaining secure operations.

"In the case of a sensitive event, e.g. sexual violence against a staff member, answering the question of 'what if the perpetrator of a sexual violence incident is a staff member?' in advance will help the organisation and its staff prepare appropriately for such an eventuality."

It is highly valuable when addressing more commonly occurring incidents to reflect on questions like:

- Did we respond appropriately and as best as we could to the last event(s)?
- What did we learn from the near misses and have we made changes to the way we work based on what we learned?

Before an incident occurs, and as good management practice, an organisation is advised to ensure that strong incident information management is part of the organisation's overall incident management policies and procedures. An organisation can do this by:

- Developing, implementing and regularly reviewing organisational policies and procedures. For instance, on management and reporting of incidents, including near misses, on addressing sexual violence cases or other particularly sensitive events, on data security, human resources (HR), etc.
- Choosing a recording and reporting system that allows safe management of security incident information within and outside of the organisation (see 'Objective four – Systematic recording of incidents' for more on recording systems).
- Defining a structure and identifying roles and responsibilities in incident management and incident information management for all staff and designated managers and focal points, at each level of the organisation from the field to headquarters.
- Assessing and identifying resources (internal and external) to enable the organisation to respond efficiently and effectively to any given incident.
- Orienting and training key staff on incident management and incident information management.

Organisations benefit from including clear procedures and training on incident information management within a broader incident management response. This will ensure that data is collected, analysed and reported appropriately, supporting the immediate response to the incident but also providing long-term benefits to the organisation.

See Tool 1: SIIM self-assessment grid for a self-assessment form that helps organisations evaluate their strengths and weaknesses in security incident information management.

Duty of care

Why should organisations care about security incident information management?

SIIM has four primary objectives, which are described in more detail in 'Chapter 2: The four objectives of security incident information management', but the overarching rationale for effective security incident information management is to keep staff, programmes and the organisation safe and secure. Strong organisational security risk management supports greater access to populations in need, but also allows organisations as employers to meet their duty of care responsibilities to staff.

NGOs have a legal (and arguably moral) duty of care: 'The duty of care is a legal obligation imposed on an individual or organisation requiring that they adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others."[10]

[10] Kemp, E. and Merkelbach, M. (2011). 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff', *Security Management Initiative.*

This duty of care towards staff and to non-employees over whom the organisation exhibits a degree of control[11] requires NGOs to put in place strong security risk management systems and processes.[12] This obligation includes implementing strong security incident information management.

A good and effective security incident information management system will support:

- a better understanding of the threat environment and the development of pertinent preventative and/or protective risk treatment measures;
- the documentation of organisational knowledge; and
- a better knowledge and understanding of the trends in the sector and community practices, particularly in relation to security.

In the event of a significant deterioration in the level of security, particularly in conflict and post-conflict environments, it is imperative that organisations have procedures in place that allow them to demonstrate duty of care for their entire staff and those they are responsible for.

> *"If incident management can be seen as a crucial learning tool when it comes to security risk management, incident information management becomes the best way to demonstrate the organisation's maturity in event analysis and decision-making. Thorough data collection, analysis, reporting and recording of incidents that an organisation experiences, and how it addressed them, could be a vitally important part of an organisation's defence, should an incident occur and a legal case be taken again them."*

Case Study: Dennis vs Norwegian Refugee Council (NRC) 2015

In what has been deemed the first test case of duty of care within the aid sector, Dennis vs Norwegian Refugee Council highlights some important lessons for security incident information management.

Summary of the facts:

On 29 June 2012, Steven Dennis, an employee of NRC, was injured and kidnapped, along with three other colleagues, following an attack during a VIP visit to one of the refugee camps in Dadaab, Kenya. Four days later the hostages were set free during an armed rescue operation carried out by Kenyan authorities and local militia. Three years later, Dennis submitted a claim at the Oslo District Court against his former employer, the NRC, for compensation for economic and non-economic loss following the kidnapping. After a careful review of the facts surrounding the case, the court ruled that the NRC had been grossly negligent and ordered the organisation to compensate Dennis.[13]

Lessons learned:

The NRC's security plan, which relied upon information from internal as well as external sources and incidents, indicated that the risk of kidnapping was high. Its analysis also indicated that international staff were at a higher risk of kidnapping than national staff.

[11] Including consultants, visitors, volunteers, etc.

[12] Kemp, E. and Merkelbach, M. (2016). 'Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications', *EISF*.

[13] Kemp, E. and Merkelbach, M. (2016). 'Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications', *EISF*.

This information was used to put in place effective risk treatment measures, including the use of armed escorts and restricting VIP visits to the area. The NRC, however, changed the security procedures prior to the VIP visit based on a re-assessment of the risks. Based on evidence provided, the court found this re-assessment unclear and unwarranted. Essentially, the information on which the security decision was based was deemed to be weak and in contradiction with previously recorded robust security information.

The NRC argued that the risk of kidnapping had receded due to there having been no kidnapping incidents in the area for the preceding nine months. The court, however, reasoned that the absence of incidents does not necessarily mean that the risk was gone, but could equally be attributed to strong risk treatment measures, not least of which was the absence of VIP visits and the use of armed escorts by almost all NGOs operating in Dadaab at the time. A better analysis of the non-incidents could have helped NRC to identify the actual – rather than the perceived – risk level.

Once the incident took place, the NRC restricted the amount of information it shared in relation to the incident with staff affected and involved. It has been argued that this lack of transparency on behalf of the organisation played a strong role in Dennis's decision to take the NRC to court.

Stronger security information management in this case might have caused the NRC to make different security decisions in relation to the VIP visit, which might have prevented the incident from occurring.

If the incident had still occurred, however, documentation of robust security information used to make security decisions might have helped the NRC in defending those decisions.

A different approach to information sharing after the incident might also have resulted in a less litigious and more open discussion of failures and lessons learned between the organisation and affected staff.

Guidelines have been developed by Irish Aid to help organisations better demonstrate their commitment to meeting their legal duty of care obligations. These guidelines are intended to provide organisations with guidance on how to reach a high level of professionalism when fulfilling their mission objectives. Each topic is accompanied by key actions, indicators and guiding notes. Adherence to these guidelines should help ensure that an organisation complies with its duty of care responsibilities and demonstrates that security incident reporting procedures include the right level people, in the right manner, and at the right time.[14] The Swiss Federal Department of Foreign Affairs (FDFA), the Stabilisation Unit (SU) and Center for International Peace Operations (ZIF) have also recently released guidelines on duty of care. These can be found here.

[14] Irish Aid. (2013). *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management.* ALNAP.

CHAPTER 2: THE FOUR OBJECTIVES OF SIIM

This chapter provides an overview of the four primary objectives of security incident information management and the key steps involved in meeting them. This chapter covers:

- Objective one: Immediate response
- Objective two: Lessons learned and applied
- Objective three: Understanding the operational context
- Objective four: Strategic decision-making

- All tools are relevant to this chapter.

1. OBJECTIVE ONE: IMMEDIATE RESPONSE

This section discusses security incident information management with the purpose of informing immediate reaction and response to a security incident. This section covers:

- 1.1 Guidance on how to report an incident: what, when, how, and to whom
- 1.2 Dealing with stress
- 1.3 Security incident follow-up process
- 1.4 Communication
- 1.5 Dealing with sensitive cases: sexual violence against staff

Relevant tools:

- 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)

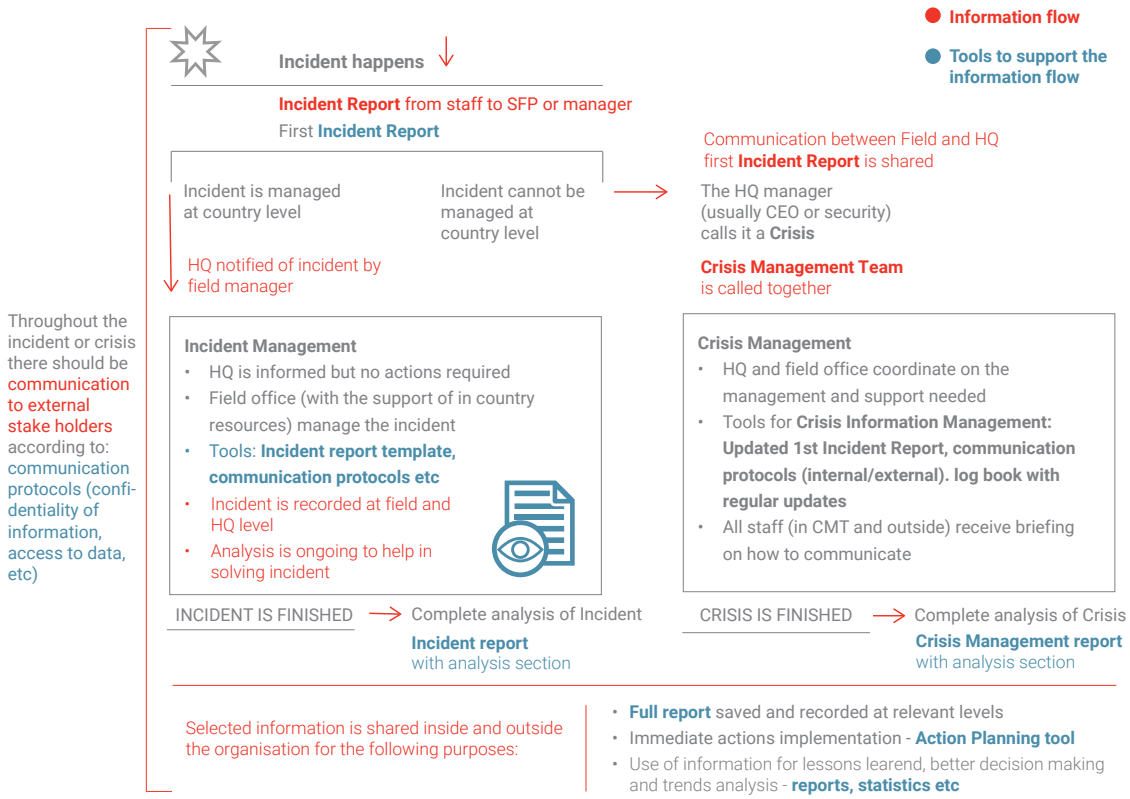
"Usually, staff involved in an incident give a first emergency call to the security focal point. Based on the information shared verbally, the security focal point provides advice and seeks basic information, such as who did what to whom, where and when. Then, when staff are safe, the incident report is filled in more thoroughly by the security focal point, using information gathered from a proper debriefing with staff involved in the incident."

One of the primary objectives of security incident information management is to inform the immediate reaction and response to an event. The purpose is to ensure that information is sought and used by decision-makers and the affected or involved staff to inform the immediate response to the incident. This usually occurs at field and/or country level, during or soon after the event.

The information recorded and reported should help identify what support is required for the affected staff and whether the organisation needs to implement any immediate changes to its operations, such as restriction of movement or temporary suspension of operations. There is a direct link between the required information and the response options that should be considered.

When an incident occurs, staff should prioritise reporting, responding and recording.

Organisations need an effective information flow that ensures that all relevant staff at headquarters, regional offices, country offices and field level are provided with the necessary information and that the information triggers appropriate response mechanisms. The following diagram[15] shows the possible flow of information through an organisation following a security incident.



15 This diagram comes from RedR UK's introductory security courses.

Necessary and appropriate information about the incident may be shared with other organisations working within the same area or country to allow them to potentially take precautionary measures to prevent the incident from reoccurring.

For security incident information management, good reporting and recording of an incident in its immediate aftermath is key.

Remember the purpose of immediate reporting is to provide staff with immediate support.

1.1 Guidance on how to report an incident: what, when, how, and to whom

Organisations should instruct staff on security incident information management and this should start with providing clear guidance on incident reporting.

> *"Often, incident reporting procedures are addressed within the SOPs section of a security plan. Some organisations have decided to develop a standalone document to cover the organisation's incident reporting policy and provide guidance to staff at all the levels within the organisation (from HQ to the field), and linking it to other policy documents (HR, code of conduct, security policy, etc.)."*

Establishing an effective incident reporting protocol allows management to:

- support affected individuals;
- discern incident patterns and trends;
- make improvements in training, procedures and physical structures; and
- allocate resources appropriately.

It is important for staff to know whom they should be reporting to, and that the incident reporting procedures outline the structure for reporting as well as what happens next. The following table delineates the key steps involved in security incident information reporting and analysis and rough timeframes for guidance.

When	Step	Actions
Right after the incident happens	Brief and chronological description of the facts.	Incident report is completed, immediate response actions taken.
	Preliminary analysis of the risks.	
Following the immediate response to the event	Factual debriefing after the incident: What are the facts/analysis to be revised/added to the completed security incident report after the introduction of new elements/ information?	Modifications to be made to the security incident report(s) already submitted incorporating new information. Action plan is designed. SOPs are re-evaluated. Feedback provided to person reporting incident and other affected staff on actions taken.
	New analysis of the risks, e.g., human, financial and material assets, operational, legal, image/ reputational, etc. and actions undertaken or to be undertaken in order to reduce these risks.	
In the weeks following the incident	The security focal point or responsible manager ensures actions are taken and determines if previous analysis was accurate.	Incident reports are updated if necessary. Action plan is reviewed, either considered as achieved, or a new one is developed. Any updated SOPs remain in place or revert to previous conditions.
	A decision is taken to decide whether the incident is 'closed' for the purposes of incident management. If not, a further plan of action should be developed.	

What to report

Most organisations use a broad definition of security incidents for reporting purposes. It is important that this definition is standard across the organisation to provide consistency, and it is important to include all incidents: critical, non-critical, and near misses. See 'Introduction – Key definitions' for definitions related to security incident information management.

An organisation can be affected by different types of incidents that are not directly linked to security issues (e.g. health and safety). The organisation must decide if these cases should be reported and recorded through the same mechanisms. If not, it should be made clear to staff what the alternate process is for health and safety incidents. If they are combined within the same recording system, a clear indication in the form of data labelling showing which category each event falls into should be included to allow analysis to focus on all or just selected categories of either security or health and safety.

"If in doubt, the incident should be reported to the security manager, security focal point or head office. These staff members will decide how to follow up on the incident."

It is not possible to define the whole range of situations that may constitute a security incident. The term is, therefore, defined very broadly and includes, but is not limited to:

- all crimes involving the organisation's personnel and property (e.g. theft, burglary, robbery, carjacking, kidnapping, etc.);
- all instances where the organisation's personnel are threatened with weapons or with acts of violence;
- all instances of harassment or threatening behaviour of any kind;
  acts of war and armed conflict such as shelling, mines, gunfire or military aggression;
- looting, attacks on property and vandalism;
- all cases in which the organisation's personnel may be involved in unlawful activities;
- all breaches of the organisation's security regulations;
- all cases of attempted bribery against organisations for access to locations, roads or affected populations, whether successful or not;
- internal threats and cases of fraud within an organisation.

It should also be made clear when reporting should happen for incidents that occur outside office hours for national staff or in personal time for international staff. Good practice would involve the reporting of all incidents even outside normal duty hours as this improves context analysis. In these circumstances, however, reporting procedures may be different.

"Give examples of security incidents which should be reported, that will help staff to identify what constitutes an incident. Categorisation is not necessary at the beginning of the process but it will help staff to understand if they should report. People need examples that are relevant to their area of operations. You can also decide to regularly discuss a category of incident that is not well-known with team members. Case studies are plentiful."

For a full list of types of incidents see Tool 2: Typology of incidents.

Organisations need to make clear to staff whether incidents reported should also include those that are external to the NGO, i.e. that impact other organisations. Organisations will often focus on the reporting and recording of organisational incidents (i.e. incidents that have a direct impact on the organisation, its staff, properties and reputation) and not include external incidents in their reporting and recording system. External events are usually monitored at field level in order not to miss important contextual information, but the organisation needs to define what constitutes an incident that affects the organisation, and the procedure to follow when formally reporting external events. This being time-consuming, it is possible for organisations to rely on external bodies working for the NGO community to record and report on external events.

"Often, it is the field mission's responsibility to track and record these types of incidents, as part of their risk assessment indicators, and they are not recorded in the global organisation's statistics."

See Tool 3: Organisational or external incident.

When reporting an incident, a template helps to ensure consistency in reporting. This template can be in a Word document, a spreadsheet, an online platform, etc., and should cover:

- author(s) of the report (including contact details, position(s) and date);
- what has happened (description and type of incident);
- victim(s) (national, international, gender, age, etc.);
- type of work being undertaken;
- when the incident occurred;
- where the incident occurred;
- whether the incident was accidental or deliberate, and specifics, particularly in-case of the latter;
- decisions taken, follow-up actions (implemented or recommended) and analysis.

If an incident requires an urgent response, guidance can be given to staff to ensure they prioritise the '6Ws':

- who is involved;
- what happened;
- where the incident occurred;
- when the incident occurred;
- what you have done about it;
- what help is needed.

See Tool 4: Incident reporting template, which looks at the most immediate information requested for security incident information management and preliminary analysis.

See Tool 5: Incident analysis grids for further questions and items that can be added at a later stage to assist with in-depth analysis.

Consistency in security incident report writing can be improved through training for staff. The following guidance on how to describe an incident can be made available to staff along with an incident reporting template.

Language	Use terms that are specific and clearly describe the behaviour that occurred. Be specific about details and do not assume that other people will understand generalities. For example, avoid using words such as 'aggressive', 'upset', or 'agitated'. Instead, state the behaviour that you observed that made you believe the person was being aggressive, upset or agitated. Remember that the description of the incident is what other people will rely on to obtain information concerning the individual(s) involved and the incident. It is important to ensure that the report does not convey negative images of those involved. The report has the ability to influence others, so care should be taken to ensure it is properly prepared and provides a factual account of the incident. Review your report prior to submission to ensure that you have not used judgmental terminology or left any unanswered questions.
Reliability of observation	Would other people who hear or saw the incident agree with the account that you have written? If another person was involved in the incident or witnessed it, it is advisable to consult with that person to ensure that the report concurs with that person's observations. Different people will have different perceptions of an incident and if some people's views are ignored it can be negative. Also, it is important to note that individuals' memories will change over time.
Objectivity	When writing a security incident report on a current event, every effort should be made to be as objective as possible and avoid being influenced by an earlier situation. As the author of the incident report, you are writing it as a recorder and not as a judge. Consequently, be sure that the report is free from judgmental statements, sarcasm, or condescending comments.
Cause of incident	If you do not feel that you have factual information, you may state your opinion provided that you clearly distinguish between opinion and fact. Even if the actual cause of an incident remains unknown after you have attempted to determine it, you should provide as much information as you have concerning what happened prior to or during the event, as this may provide a clue to the reader. If you did not actually witness the incident or event, you may still write an incident report, however, be sure to state that the information is based on what was reported to you and by whom it was reported.

When to report

The timing and level of detail of reporting depends on the category of the incident:

- **Incidents requiring immediate action** should be reported immediately with the purpose of asking for support and additional instructions. Critical incidents that pose significant and/or an ongoing threat to the organisation's personnel, property or programmes are generally deemed urgent for the purposes of immediate reporting and response.

- **Incidents where no immediate action is required**: Incidents or near misses that reflect insecurity or a change in the threat environment, but do not pose an immediate risk to the organisation's personnel, property or programmes, tend not to be urgent for the purposes of reporting and could therefore form part of a scheduled daily or weekly report to a line manager or SFP.

Incident reports may be completed at a number of stages as more information becomes available.

Immediately: immediate incident reports are made as soon as it is safe to do so, often by radio or phone. A situation may be confusing initially, so time should be taken to assess what has just happened, how safe staff and others involved are, and what assistance is needed. When reporting an incident over the phone or radio, staff should speak clearly, accurately and concisely. If it is not possible to provide full details (because of shortage of time, or because it is unsafe to do so during an ongoing incident), provide whatever information is possible, in order to trigger the appropriate response. Even the briefest sharing of information couldsave lives.

Staff who are likely to receive immediate incident reports (such as radio operators, line managers and SFPs) should be trained in how to respond. Knowing what questions to ask and being empathetic to the reporter can have a big impact on the effectiveness of the response and the recovery of the impacted individual(s).

In the following hours and days: Some incidents may require one or more follow-up incident reports. These can be made as often as necessary, with the frequency and level of detail determined at the outset and revised regularly. In an ongoing security situation, the SFP or designated authority should maintain a daily log of activities. Not only will this help maintain a record of decisions and activities for the improved management of the situation, but will also provide the information needed for updates and ultimately support organisational learning. Information should be shared in writing where possible, to reduce the risk of miscommunication and misunderstanding. This also helps individuals under stress better frame their thoughts. See the section below on 'Dealing with stress'.

Once the incident has stabilised or is 'closed': Some incidents may require a full/final security incident report, usually in written form. As soon as it is appropriate to do so, those involved will be required to provide a written account of the event and the actions that were taken,. Where the field office needs to take specific steps to treat risk, including making corrections to existing procedures, training, resource allocation, etc., these follow-up measures should be clearly stated, the individual(s) responsible for implementation identified, and the time-frame specified. Subsequent follow-up reports should record the progress of recommended actions until their completion. The full

incident report should form the basis for re-assessing or updating the organisation's relevant SOPs. This will be discussed further in 'Objective two'.

Staff should be made aware of what to expect and what to ask for when they report an incident. Triggers should be clearly identified and responses clearly explained in advance. To reduce under-reporting, the procedure should be clear but flexible: reporting can be simple, or can become more thorough when required.

Whenever possible, it is best to prepare an incident report immediately following the incident while the facts are still clear. However, and depending on the severity of the event, staff may still be emotionally involved at that time so it may be helpful to have another person review the report prior to it being submitted.

How to report

Incident reporting procedure should identify the safest means of communication, taking into consideration the three different moments of reporting.

Incident reporting procedure should clarify whether radios, satellite phones or emails should be used and ensure staff are trained on using devices safely and securely (using encryption if necessary). Staff should be made aware of the need to ensure confidentiality around reporting incidents.

The reporting procedure should also clarify the differences in channels for reporting different types of incidents. For example, a burglary and an incident of sexual violence will require different reporting mechanisms. Incidents that require an administrative response, e.g. insurance claims, replacing assets, etc., may also require a specific procedure. See 'Dealing with sensitive cases: sexual violence against staff' in this section below for more information on reporting sensitive cases.

It is possible to develop different processes for incident reporting depending on the nature of the incident, i.e. level of confidentiality and sensitivity required. Nonetheless, it is important to emphasise that the channel should usually not be the most important consideration (unless there are serious interception or privacy concerns). Particularly for incidents that require an urgent response, what matters most is that the information passes through to the intended recipients as fast as possible so those affected get the support they need.

It is also crucial that staff respect confidentiality of information internally, to ensure there is no interference with the management of the event. Focal points can use the 'Categories of information' table in 'Objective three'.

Whom to report to

All staff should be able to report an incident and the organisation's incident reporting procedure should make it clear to whom staff should report incidents. For example, this can be via email to a particular individual or through an automated online reporting system that automatically sends reports to relevant staff members within the organisation.

The following table provides examples of individuals and their corresponding tasks and responsibilities in the event of an incident.

Who	Tasks and/or responsibilities
All staff	Should report the incident to their manager or the designated security focal point.
Security focal point (at field or country office level) Manager (at field or country office level)	Upon receiving the initial incident report should ensure support is provided to the affected staff, inform the country/regional office should support be required, follow up on the incident and arrange a debriefing on, and analysis of, the incident. Should suggest immediate operational measures to regional manager. Ensure communication to field staff if necessary.
Country or regional security focal point Manager (country or regionally-based)	Upon receiving information from the field or country office, should ensure support to affected individuals, relay to HQ information should support be needed, ensure follow-up and potential debriefing should staff be removed from the field location. Discuss and agree on potential immediate operational measures with the country or field manager.
Security manager or advisor (at HQ level)	After receiving information from the regional or country office, should ensure support from HQ is provided if required. Will liaise with decision-makers at HQ level to validate the appropriate level of management.
Manager and executive director/ chief executive officer (CEO) (at HQ level)	Will receive incident information from the security manager/ advisor at HQ level and/or managers at the regional or country level. Should ensure follow-up of specific actions at HQ level, if these are required. Ensure communication about the incident to HQ level staff should this be necessary.

The information flow related to an incident needs to be adapted by each organisation to reflect staff positions, hierarchy and operational presence.

Responsibilities of staff for security incident information reporting and management should be clearly identified in policy documents (e.g. security risk management policy, incident reporting policy, Code of Conduct, etc.) and procedural documents. The roles should be highlighted during the induction process and regularly throughout the employment cycle.

1.2 Dealing with stress

Staff who report an event while it is happening it or immediately afterwards are likely to be under significant stress. It is recommended that staff who receive the first verbal report endeavour to:

- remain calm;
- identify the person who is making the report;
- ensure the safety of those involved in the incident;
- prioritise information required, e.g. status, what has been done, what needs to be done immediately;
- collect information according to the incident reporting template;
- reassure the person reporting the incident and agree on further communication.

The purpose of this first report is to obtain the necessary facts to inform an immediate response. This is not an emotional debrief (often called defusing). Psychological support and an emotional debrief for individuals following a traumatic event should be done by professionals when required. This emotional debrief (or defusing) is mostly relevant for critical incidents, but some non-critical incidents will also have traumatic effects on the person involved. The organisation should ensure support is given to staff in both situations.

1.3 Security incident follow-up process

All security incidents should be followed up to ensure that all the information related to the incident is captured to inform lessons learned, context updates and decision making.

The incident follow-up process provides incident report updates depending on new or emerging facts. It is also a very useful process to go through when there are staff changes in key relevant positions, e.g., the security focal point. In certain instances, this may require a new version of the incident report to be developed.

This process should capture every new event or new action realised during the management of the incident, until the incident is concluded and closed.

Critical incidents, such as staff abduction, can continue for a long time, with new information becoming available sporadically. It is important that the organisation captures this new information in a meaningful way so it can be analysed and accounted for in the decision-making process. This should form part of the crisis management plan.

Follow-up processes should be defined for all incidents, to ensure the information and lessons learned are not lost or de-prioritised in changing environments.

Factual debriefing

A factual debriefing should come after the involved staff have received the appropriate support following an incident. It is recommended that this debriefing happens within 48 hours of a security event. The extent of the debriefing will vary depending on the nature and complexity of the incident.

When organising a factual debriefing for information collection purposes, it is important to keep basic principles of Psychological First Aid (PFA)[16] in mind:

- conduct a debriefing only after the individual's basic physical and psychological security have been ensured;
- the debriefing should take place in a safe space;
- aim to empower the individual affected;
- be clear about the process, expectations and follow-up actions.

It is important to remember that the impact on specific staff of near misses and small incidents may be much more severe than the impact on the organisation. For example experiencing harassment by community members or a failed mugging can affect an individual profoundly.

[16] For further information on PFA, see guidance from the World Health Organisation (WHO) here.

See Tool 6: How to conduct a factual debrief for further guidance on how to organise a debriefing for the purposes of information collection and analysis. Please note, this is not an attempt to train readers on PFA or on how to become professional investigators. It is a list of tips to conduct safe and useful fact-finding interviews for incident reporting purposes.

Information sources
Information gathered should be verified for its accuracy by talking to internal and external stakeholders to gather different perspectives, i.e. to triangulate information gathered.

A critical element when analysing security information is the credibility of the information and validity of the source.

The following reliability and validity matrix[17] is a simple tool that can assist with this verification process.

Source reliability

	Rating	Description
A	Completely reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually reliable	Minor doubts. History of mostly valid information.
C	Fairly reliable	Doubts. Provided valid information in the past.
D	Not usually reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History of invalid information.
F	Reliability cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

Information validity

	Rating	Description
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably true	Logical, consistent with other relevant information, not confirmed.
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Truth cannot be judged	The validity of the information cannot be determined.

[17] United States Army. (2006). *Field Manual No. 2-22.3*. Human Intelligence Collector Operations.

For example: an A3 rating is from a very reliable source but the information is only possibly true. Whereas, a D1 rating is that a usually unreliable information source has provided confirmed information (verified by other sources).

This matrix is easier to use if an organisation has an updated stakeholder mapping. Source reliability is something to be observed over a long period of time; the SFP should regularly cross-check any operational information provided, to assess the reliability of sources and the validity of information received.

Organisations may receive security information from other NGOs or individuals in an indirect manner, through a third party or by bypassing the usual stakeholders. This is sometimes referred to as diagonal information flow. For example, witnesses to the carjacking of an NGO vehicle with no means to contact the organisation directly, called the consortium instead. The consortium relayed the message to the security director of the NGO, who in turn relayed the message to the country office in the field.

1.4 Communication

A policy should be developed at an organisational level to outline what security information should be shared and with whom, both externally and internally and in particular, immediately after an incident, and to identify the person responsible for sharing information across the different levels of an organisation (from the field to HQ) and externally. The policy should cover confidentiality issues in order to protect the identities of affected individuals and other relevant stakeholders as necessary.

It is recommended that one focal point from each necessary level within the organisation (from field to HQ) is identified as being responsible for external communications, to ensure it is done well, and in a timely manner.

"The ethics of using privileged information in conflict zones while managing security incidents should be addressed. A security focal point should be able to filter specific information for purposes of ethical adherence, while effectively disseminating relevant information to further ensure the safety and security of staff and the organisation's mission."

Coordination mechanisms can be used by organisations to collect information and feed it into their context analyses and incident management, both through formal procedures as well as by improving informal professional relationships with key actors.

The team leader or SFP should determine the level of information to be shared within and outside the organisation, in accordance with the policy.

Communicating with authorities
For many incidents, it may be appropriate to share what is known with the police or other law enforcement agencies, especially during a critical incident such as bombing, attack, kidnapping or assault, in order to help solve the incident, to reduce its impact, and/or to reduce the likelihood of similar events affecting others.

Agreement and collaboration with the host government is often a key component of effective NGO operations. Therefore, in some contexts, organisations are strongly advised to report incidents to local authorities and the police. Nonetheless, this reporting should be done on a contextual basis, considering a variety of factors, and should be considered before an incident happens and be included in the organisation's SOPs or contingency plans.

Communicating with the media

High-profile or critical security incidents can attract extensive attention and pressure from external sources, particularly the media. Other incidents can also interest media outlets, depending on their agenda (e.g. trends for publications, etc.).

The primary concern should always be the security of individuals directly affected by the incident and the well-being of their colleagues and families. The sharing of some information may endanger lives. However, the speed with which the right information travels can save lives. The way in which an organisation responds, not only to the incident but also to information and opinions about it, is important for the safety of staff and the organisation.

Remember: once information is in the public domain it cannot be retracted, whereas additional details can always be released later.

Key organisational tasks should be adapted to the scale of the incident being dealt with and responsibility for them should be assigned during the planning phase. See the following table to guide staff who are responsible for preparing an organisation's external communications security strategy, particularly in relation to dealing with the media:

	Make sure you are in control of your information.
	Continue to monitor information available on the event from all sources.
	Prioritise monitoring of social media to remain aware of information that is available about the incident in the public domain. Monitor local language sources as well as HQ language and others as appropriate.
	Identify or pre-identify a spokesperson.
	Seek to prevent publication. If this is not possible, correct and/or remove problematic stories, messages, images and film from any source. Explain that this is because media attention can endanger staff.
	Ensure incoming media phone calls are logged with date and time and referred to the lead spokesperson.
	Prepare key messages and FAQ answers for lead and/or additional spokespersons.
	Brief and rehearse lead/additional spokespersons.
	Draft a written statement to be read by the spokesperson if necessary; this helps to ensure people stay on message.
	Stick to facts and do not offer 'off the record' information.
	Align internal and external communication.
	Record decisions made and the factors that influenced decision-making.

	Make sure the NGO is seen as a credible, authoritative and reliable source of information.
	Tell the truth, avoid using 'no comment'. Do not speculate. If a response is required but information is limited, issue a holding statement.
	Respect journalists and their deadlines and return media calls. Invite media callers to consult the NGO's website or social media accounts for updates, e.g. Twitter.
	Offer to include media callers in the agency's email listing, making sure they get any news and press releases uploaded to the internet.
	Use tools such as Twitter to release information in brief, with links to the website where statements and press releases can be read.
	Ensure all staff who have outward facing roles (such as guards and drivers) know the appropriate response to any questions and whom to direct queries to.

	Always bear in mind the main objective is the safety and protection of staff directly affected.
	Do not disclose any personal data of individuals affected by or involved in the incident.

See EISF guide 'Managing the message' for additional guidance and tools, including a holding statement template.

Collaborating with other agencies

A major part of the overall security posture for any aid organisation should be close cooperation and information sharing with other agencies and NGOs operating in the same area or areas deemed operationally relevant.

Coordination in communication is particularly relevant when a security incident involves a group of individuals from different organisations. Anticipated coordination will be key in the immediate response, and consistent and coordinated incident management and incident reporting should be discussed and agreed upon in advance. This can be addressed in specific SOPs.

When security incident information is not collected, managed and disseminated horizontally, the threat image of a region is difficult to ascertain. Security collaboration mechanisms thrive when both vertical and horizontal communication continually 'close the loop' (i.e. provide feedback) and when stakeholders work in a coordinated fashion.

An incident debriefing with other relevant organisations should quickly follow security incidents, if information sharing is deemed appropriate.

The incident reporting form could be used as a guidance document to develop a debriefing. SFP and/or relevant managers should identify in advance the most relevant data/information that can be shared with other organisations. These decisions should take into consideration, however, the category of information the various parts of the incident data fall under (see 'Objective three').

Key elements in the incident debriefing should focus on clarifying: who did what, where and when. In the interests of protecting affected individuals, organisations should not disclose who was involved. However, if ethnicity, nationality or other personal factors are considered fundamental, consider how this information can be shared while maintain confidentiality. Building trusted relationships before an incident happens is essential for sharing nuanced information.

A debriefing can also be viewed as an opportunity to seek support from other organisations, be it logistical support, assistance, improved coordination and sharing of information or, in more extreme circumstances, taking a political stance together as an NGO community on a particular issue (see 'Objective four').

As always, the decision to share information should consider any possible impact on the security of the organisation's staff and other affected individuals.

When an organisation receives security incident information from another organisation, specifically around critical incidents, it is advisable to:

- Avoid contacting the NGO leading the incident management (if the incident is ongoing), unless there is relevant information to be shared that can help them respond to the incident.
- Avoid any type of interference unless asked.
- Do not share the information further (the affected NGO decides who should be made aware).
- Evaluate the need to implement specific measures to reduce the organisation's exposure to a similar event, communicate this need with key internal stakeholders and implement the risk treatment measures identified.
- Define what information is needed to explain the above measures (if necessary) without disclosing confidential information.
- Try to reduce the possible rumours within the organisation by addressing questions and requesting staff to maintain confidentiality.
- Evaluate the need to review and update security measures for the organisation.

Organisations in a similar area should use collaborative mechanisms to share information that would be useful to other organisations in the assessment of a security context. This structured type of information sharing across different organisations is discussed in more depth in 'Objective three'.

1.5 Dealing with sensitive cases: sexual violence against staff

Some incidents have to be approached sensitively and with special care, particularly when it comes to the management of security incident information. The impact of these incidents can have special ripple effects for those involved, the organisation, and the broader humanitarian and development community.

In this section, we are referring to security incidents that are often considered to be especially traumatic to the individual(s) involved. For the purposes of clarity, we will use the specific example of sexual violence against aid staff, though the principles and management approach outlined in this section could be applicable to other types of

situations, including kidnappings or the murder of staff. Guidelines in this section should be used in conjunction with the rest of the handbook, and users should reflect on the survivor-centred approach.

Evidence gathered by Report the Abuse[18] suggests that sexual violence, which ranges from sexual harassment to rape, occurs in NGO workplaces and that the majority of perpetrators are colleagues of the survivor. Female aid workers are particularly at risk, although men can also experience sexual violence.

A report published in 2016 on this issue found that only 16% of humanitarian NGOs assessed had a single mention of sexual violence as being a risk to staff within their policy and procedures, let alone comprehensive, sensitive, or survivor-centred response mechanisms.[19]

Developing an appropriate security incident information management system that incorporates information about sexual violence against staff will be a big step towards the development of better prevention and response strategies.

Sexual violence against aid workers is a serious threat that not only undermines the safety and security of programme staff members, but can also significantly degrade the effectiveness and efficiency of NGO operations. It is important to consider sexual violence as a violation of rights, which means a protection dimension is directly applicable to the management of such cases.

Under-reporting – reasons and obstacles

Sexual violence is under-reported in every context, country, and culture. There are many reasons why incidents of sexual violence might be under-reported in the humanitarian context:

- Lack of knowledge about, or absence of, channels or procedures for reporting.
- Lack of organisational investment in training and knowledge needed to receive reports of sexual violence.
- Limited evidence or legal recourse, or concerns that reporting the incident will not result in justice or retribution.
- Concerns about discriminatory labelling, victim-blaming or rape myth responses from the organisation and colleagues.
- Socially ingrained shame, guilt, or humiliation about having experienced sexual violence.
- Fear of retaliation, professional or personal consequences.
- Lack of trust in the system.

These are all serious reasons why an individual might not report, and organisational structure and culture underpin most of them. Every NGO should reflect on the culture that it is creating, and whether it is accessible, communicative, open to constructive feedback, trusted, sensitive, and survivor-centred. Engaging staff at all levels in productive and safe discussions around this issue can considerably shift some of the concerns that lead to under-reporting.

[18] See the Report the Abuse website for more information: http://reporttheabuse.org/about/

[19] Nobert, M. (2016). *Prevention, Policy and Procedure Checklist: Responding to Sexual Violence in Humanitarian and Development Settings*. Report the Abuse.

"At the moment, there are no good practices that NGOs can follow in order to prevent sexual violence in their workplaces and ensure that they comply with the duty of care they owe to their staff. Detailed guidelines on how to respond when an incident does occur are also unavailable. Report the Abuse, however, is in the process of developing such good practices, with the first tool slated for publication in Spring/Summer 2017."[21]

Important considerations regarding sexual violence and SIIM:

- Informed consent: at all stages in the collection and use of the information a survivor provides about an incident, their informed consent must be obtained.
- Training on sexual violence incident reporting and management: knowledge about how to receive information about an incident of sexual violence and how to respond appropriately can significantly reduce re-traumatisation and create trust in an organisation's reporting structures.
- Providing clear definitions on sexual violence: informing staff of the meaning of, for example, sexual harassment or sexual assault will help to establish a clearer policy.

See Tool 2: Typology of incidents for definitions in relation to sexual violence.

Immediate response

When an incident of sexual violence has been reported, or brought to the attention of the organisation by a third party, the first course of action should always be to ensure the survivor is in a location where they feel safe, and that their physical and emotional needs are being addressed. Once this has been established, there are a number of recommended actions that should be taken to ensure that information about the incident does not become rumour, escalate a situation, or place the survivor and other staff in danger.

Appointed focal points are advised to take the following immediate actions:

- **Clarify next steps:** Clarify with the survivor what course of action they would like the organisation to take. This position should be routinely checked to see whether the survivor is still comfortable.
- **Confidentiality:** Ensure that other staff members who know of the incident do not speak about it to those who do not know. It is advisable to give them a standard response if questions are asked, e.g. 'I cannot answer this question, please contact the resident representative.'
- **Communications:** Establish a direct line of communication with a designated focal point at headquarters. Communications between the field and headquarters should be managed and controlled by only those designated on the ground. This communication should not involve a series of intermediaries or many alternates. The situation should not be discussed where such discussion can be overheard.
- **Media management:** Take proactive action towards the media if it looks like the incident will get press coverage, persuading editors and journalists to use at most only the initials of the survivor, and not their full name. It is advisable to agree upon a code name, a code word or a case number to refer to the survivor.

[20] More guidance on the contents of this tool, and how Report the Abuse is helping humanitarian organisations to address sexual violence in their workplaces can be found by visiting their website or reaching out directly.

Any actions taken regarding the press must be thoroughly discussed with the survivor in the event that they would be identifiable.

- **Report management:** Reporting lines should be clearly identified before an incident occurs, and then followed when a report is made. This must include alternative lines of reporting at the field level, ensuring that there are multiple individuals to whom reports can be made, of varying genders, sexual orientations (where possible), and cultural backgrounds. These individuals must have appropriate training to receive reports of sexual violence. There should also be reporting lines that bypass the field level, for situations where senior management in the field may be implicated or not trusted to appropriately address an incident of sexual violence.
- **Management decision-making:** due to the sensitivity of information, specific measures must be put in place to ensure that statistics on sexual violence incidents are not lost so mitigation and management measures are included at all levels of an organisation's security policy and practice.

Information on how and to whom to report should be made widely available in simple and clear language in various places throughout the operations of the organisation. This can include placing paper copies of the process in every field office, ensuring it is accessible to those without access to computers. Furthermore, information on the reporting process should be made available in all relevant languages for the operating environment. If literacy is a concern, creative means should be employed to ensure everyone understands their rights and how to react if sexual violence occurs. When developing reporting systems, these must recognise local cultural norms and may be different for different staff, e.g. national and international.

Collection of information

Following an initial report, additional information relating to the incident should be collected. Collecting necessary security information in these circumstances will likely require special training and skills for the incident to be addressed sensitively, professionally, and comprehensively, in a way that does not add harm to those involved.

The following tips provide guidance to staff collecting information in relation to an incident of sexual violence:

- When seeking information from the survivor about the incident, go slow and allow time for breaks and the gathering of thoughts. Begin with broad open-ended questions until a complete outline of the events has been stated once. Questions for specific details can follow once a broad explanation has been provided.
- Be cognizant of the fact that requesting this information can be re-traumatising for the survivor. You can make this process easier by providing the time and space needed for the survivor to talk about their experience, by providing a safe and encouraging location and atmosphere, and by being an empathetic and active listener.
- Questions should be asked in an environment where the survivor feels safe and comfortable. The option to be accompanied by a colleague, friend, or trusted focal point should be respected and encouraged. While it might seem like a small gesture, ensuring there are items such as water and tissues present will help to create a climate where the survivor feels supported.

- Do not ask questions that perpetuate rape myths or victim-blaming attitudes, such as: 'are you sure this is what happened?', 'what were you wearing?', or 'what did you do to cause this event?'
- Where possible, collect the survivor's clothing or any other items that might help to prove in a court of law that sexual violence occurred. These items should be stored in as clean and careful a manner as circumstances allow.
- If the survivor has not showered or cleaned themselves, encourage them to seek medical care, if this is available, including the consideration that they may want to take a morning after pill or post-exposure prophylactics (PEP). Ensure SOPs include access to and use of morning after pill and PEP.
- After asking questions of the survivor, ensure that they are going to be in a safe location with adequate support afterwards. While your role may primarily be to ask questions, you should nonetheless confirm that they have access to necessary psychosocial support or avenues to accessing these support structures, and if necessary take steps to ensure this is provided.
- Assure the survivor at all stages in the questioning that they are believed, that they will be informed of all next steps, and that they did not deserve or cause what happened to them.
- After relevant details of the event have been collected, ensure this information is securely stored in a location where it will not be accessible or leaked. Where possible, use code names, code words or a case number to refer to the survivor, even in internal communications.

We tend to assume that someone might be more comfortable communicating with an individual of the same gender, however this is not always the case and options should be provided. Such options should include, where possible, diversity of sexual orientations, nationalities, racial backgrounds, religions, and other diverse profiles.

It is worth noting from the outset that the collection of incident information regarding sensitive situations, as well as the reporting of such incidents, must protect the identity of those involved, without compromising information sharing and the safety of the broader humanitarian and development community. When it comes to reporting, there is also a fine line between maintaining confidentiality about the incident, the survivor's identity, and sending the message that survivors should feel ashamed about their experiences. By employing a sensitive survivor-centred approach, it is possible to reduce the chances of crossing over this line.

It should also be noted that hearing about sensitive incidents can be as triggering for the individual collecting the information as it is for the one who survived the incident. Vicarious trauma may occur and psychosocial support should be provided if needed.

See Tool 7: Good practice in gender-sensitive incident reporting and complaints mechanisms for reporting sexual exploitation and abuse (SEA).

Where there is a possibility that the safety and security of other NGO staff at field level is, or will be, compromised, information about the incident should be shared appropriately with other organisations, or through networks such as the United Nations Department of Safety and Security (UNDSS) or NGO security forums. The survivor must give their informed consent to this sharing of information, and their role in ensuring this event does not happen to others should be highlighted.

2. OBJECTIVE TWO: LESSONS LEARNED AND APPLIED

This section discusses security incident information management with the purpose of collecting data, processing and analysing it, transforming it into useful information, extracting lessons from the incident and implementing follow-up actions. This section covers:

- 2.1 Post-incident analysis
- 2.2 Implementing lessons learned
- 2.3 Analysis and follow-up actions of sensitive cases

Relevant tools:

- Tool 2: Incident analysis grids
- Tool 8: Action Plan

The second primary objective of security incident information management is to implement lessons learned after a security incident for follow-up action and prevention.

The purpose is to understand what happened with a view to planning and implementing any necessary changes and procedures that will help to prevent, treat the risk or lessen the impact of similar events. This usually occurs at country/headquarters level shortly after the security event.

An incident review should be carried out within the organisation after the incident is considered 'closed'. An incident is usually considered closed by an organisation when the required reporting, learning and updated protocols have been carried out, and the incident has stopped evolving. Defining the status of an incident supports analysis.

Incident status vs incident management status

Organisations benefit from defining a list of incident statuses that will be applicable to events and their management. This supports the incident information follow-up process and particularly post-incident analysis:

- Incident status:
  - Ongoing: still happening.
  - Concluded: the main event is deemed 'over' by the organisation.
- Incident management status:
  - Open: main incident is finished but management of impact and its analysis is still ongoing. The incident is under investigation.
  - Closed: when all lessons learned and actions taken are implemented.

For long-running incidents, such as abduction, it is useful to carry out an intermediate 'real-time' review of actions taken after the initial event so that these learnings are not lost.

Post-incident analysis can be conducted with staff directly affected by or involved in the responses and the organisational decisions that may have contributed to influencing how the incident occurred.

This requires an analysis of qualitative information for a frank assessment of contributing factors that increased vulnerability and influenced the specific reactions that occurred as the event unfolded. The information gathering process should be conducted in an atmosphere of confidentiality and trust. It is important to avoid blaming affected staff in the aftermath of an incident.

2.1 Post-incident analysis

The post-incident analysis considers how staff and the organisation were directly affected by the incident and whether they were adequately cared for. It examines how organisational policies or individual behaviour may have contributed to making the incident possible and asks whether better guidance may need to be developed. It further examines how organisational responses helped (or hindered) in mitigating or resolving issues that arose from the incident.

Analysis seeks to understand why security incidents occur and the various reasons behind them.However, this is only of value if appropriate action is taken by the whole organisation to ensure that these incidents are less likely to happen again.

It is advisable to document the real impact of the incident plus measures to be undertaken to reduce the likelihood of such an incident happening again, and the impact if it does. For critical incidents, the analysis should also involve an evaluation of the management process, i.e. what decisions were made, when, and why. The written process is imperative if the organisation is to systematically document the lessons learned from the incident and reflect this learning into future operations and policies, as well as providing evidence of organisational learning to support the organisation's duty of care responsibilities.

Some important points to keep in mind when planning a security incident analysis can be considered in three groups, as below.

The reasons for conducting a security incident analysis:

- It seeks to understand the root causes behind security incidents.
- Careful analysis is the key to identifying new or improved mitigating actions that can be taken to enhance SOPs and the overall level of security of the organisation, thus enabling improved access to populations in need.
- It helps to identify the motives behind the incident, for example, if an attack was deliberate or not. The distinction is important for understanding the operational context. If evidence indicates an incident was deliberate, it also helps to identify if, and why, the organisation was deliberately targeted.
- By including elements of analysis in each security incident report, an organisation can build up a bank of information which will support trend analysis.

An analysis of the incident should focus on the following areas:

- Leading up to the incident, were procedures followed and are changes needed?
- Was the organisation or an individual targeted? Is this because something provoked an attack? Was the affected staff member perceived as being wealthy or a soft target?
- Is the organisation no longer accepted in the area?
- What was the impact of the incident on programme activities?
- Were the procedures in dealing with the incident appropriate?

Some common contributing factors to security incidents include:

- Ineffective security risk management and/or ignorance of procedures.
- Lack of basic security awareness and training.
- Profile of the organisation in the country and how it is viewed by the local population (e.g. behaviour, cultural insensitivity, etc.).
- Interpersonal relations and personal problems (including internal human resource issues).
- Crime due to visible or perceived wealth.
- Lack of information resulting in bad security decision-making.
- Taking unnecessary risks.
- Stress-related security incidents.
- Staff pushing the boundaries, or getting too comfortable with operating in an insecure environment.

Organisations should consider if they can share with other agencies the final analysis (or part thereof) of their conclusions on the causes of an incident and how to better manage particular situations.

For further guidance, see the different tables in Tool 5: Incident analysis grids.

It is important to analyse an incident in its overall security context (see 'Objective three') but also in the light of other incidents, either in the area, or following similar patterns. This trend analysis is made possible through systematic recording of incidents within the organisation. This is discussed in more detail under 'Objective four'.

2.2 Implementing lessons learned

The most obvious benefit of gathering information from a security incident is to use it immediately for programming purposes, such as adaptation of travel plans and field trips to improve organisational security. The content of analysis will feed into determining access, the parameters of the project, implementation, with links to HR, budgeting, monitoring and evaluation at operational level.

Other examples of lessons learned from incident information include:

- Immediate changes in operations and updating of SOPs and contingency plans; looking at separate incidents together can trigger decisions at the country level.
- Development of new indicators for security context follow-up and risk assessment.
- Sharing lessons learned among offices across the globe will allow this information to feed into the periodic review of procedures, policies, and country security plans.

A good security incident analysis document will include a section for recommended actions, linked to identified causes. Good practice suggests attaching a follow-up action plan to the incident analysis report, to ensure recommended actions are indeed implemented.

Using the organisation's IT system, it is possible to link the action plan to planning tools and send automatic reminders and notifications to responsible staff.

See Tool 5: Incident analysis grids for examples of actions which can be implemented after an analysis is made in relation to the causes of incidents.

See Tool 8: Action plan for what information a follow-up action plan should contain.

2.3 Analysis and follow-up actions of sensitive cases

Analysis of an event must adhere to the following principles: confidentiality, neutrality, and professionalism.

In the event of sexual violence within an organisation, the primary function of the analysis stage, for the purposes of this handbook, is to determine what steps need to be taken, administratively or legally. This will differ greatly between organisations and operating contexts.

If it is possible to do so without exposing sensitive details about the event or survivor, consult with those in similar roles at the field level to gather information about the broader security situation and other incidents of sexual violence at field level.

Use this and any other tools to conduct security analysis to determine whether other staff members, the organisation, or the broader NGO community are also at risk of experiencing sexual violence or other forms of violence.

Analysis of these types of events should also include impact analysis, including both primary and vicarious trauma, as well as training and other reactive actions that might be needed for the prevention of such incidents in the future.

Consult with necessary focal points – at field and HQ level – to identify what follow-up actions are needed, and ensure they are undertaken. Additional consultations may need to be carried out with human resources, legal, ethical, staff welfare, or medical services, as appropriate for the organisation. Information shared should be on a need-to-know basis and steps to facilitate legal action must be taken at the request of the survivor, and with their informed consent. Whether legal action can be taken in a particular context may vary drastically, depending on an individual's profile and the legal operating environment. The needs and desires of the survivor to pursue the matter should govern any legal actions. Consult with national staff and other actors to gather angles on whether legal justice is possible in the context, and any risks the survivor might face by taking this route. In some locations, it may not be a realistic option at all, and in such instances expectations may need to be managed.

Even if it is known that someone in the organisation has experienced sexual violence, or if a survivor has taken the steps to report, there are several elements that should be borne in mind. First, coming forward to report does not automatically mean that a survivor will want the details to be widely shared and discussed. At all steps in the reporting process, the survivor should be informed about and consent to who is told about their experience. It is the responsibility of staff involved, the manager, and the organisation to protect the identity of the survivor and the confidentiality of the details of the case.[21]

[21] Van Brabant, K. (2010). 'Chapter 12: Sexual aggression' in *GPR8 – Operational Security Management in Violent Environments, Revised Edition.* Humanitarian Practice Network/Overseas Development Institute (ODI).

Should a survivor wish for their identity to be reported or shared, or for other identifying details to be shared however, this should also be respected. The survivor-centred approach to addressing incidents of sexual violence provides that the survivor's decisions and desire dictate the course of the reporting process and their care.

Information on confidentiality should be communicated to the survivor in a manner that makes it clear that while any desire to keep their identifying features contained will be respected, they should not feel that they need to do so as there should be no shame associated with having been subjected to sexual violence. Also ensure the survivor knows that they can make their identity known at a later date, should this be their choice.

What information will be communicated, and to whom, should be first discussed with the survivor, and their informed consent provided. In some instances, there is no choice but to provide details about the incident to others, but by allowing the survivor to be part of the process, we can ensure they begin taking back the power they lost during the sexual violence incident.

Only relevant details should be communicated to individuals deemed necessary, to reduce the chances of additional harm.

If necessary, to ensure the safety of other members of the organisation, information about the event might need to be shared with other employees. This should be done in a sensitive manner, protecting the survivor insofar as possible. Hearing about incidents of sexual violence can be triggering, so ensure that vicarious trauma is not being experienced by the other staff, and ensure all within the organisation have access to psychosocial support.

While maintaining the survivor-centred approach, the organisation must also find a way to ensure that the fact of these types of incidents is acknowledged at both the country and headquarters level. Sexual harassment and violence very rarely appear in country security plans or organisation risk registers, even when it is recognised anecdotally as an issue.

3. OBJECTIVE THREE: UNDERSTANDING THE OPERATIONAL CONTEXT

This section discusses the benefits of understanding the operational context and the means to do so. It highlights in particular how to collaborate with other organisations for the purposes of incident information sharing as well as resources for obtaining contextual information. This section covers:

- 3.1 The practicalities of sharing security information
- 3.2 External sharing of incident information
- 3.3 Forums for sharing security incident information
- 3.4 External contextual trend analysis resources

Relevant tool:

- Tool 2: Typology of incidents

The third primary objective of security incident information management is to understand an organisation's operational security context. Good contextual knowledge allows organisations to make sound security and operational decisions at country, regional and headquarters level. Analysis of the patterns of incidents reported by organisations are the most effective source of information on the specific security context.

To obtain the most comprehensive understanding of a context and to achieve the best strategic use of security incident information, however, security analyses should include incident information from more than one organisation and multiple sources.

> *"Information on the general security context can be obtained from various sources, among them other organisations, the media (including the humanitarian and development-focused media), and information provided by specialised services providers who can provide country overviews or risk forecasts often on a subscription basis."*

NGOs often find it useful to benchmark their incidents against comparable organisations, whether this be in terms of programmatic focus (e.g. humanitarian, development or human rights, etc.) or size (e.g. in terms of presence or staff numbers). For smaller organisations, it can be vital to have access to additional incident information from the same country before any trends can be identified.

Analysis of the patterns of incidents reported by multiple organisations is one of the most effective sources of information of the specific security context. The analytical conclusions derived from a global overview of security incidents can be used by organisations to benchmark their own trends and to inform strategies and communication within organisations and the humanitarian and development sector as a whole.

Trend analysis can also be a useful tool to inform the media and to influence public opinion and government donors.

3.1 The practicalities of sharing security information

Categories of information – from confidential to public

The sharing of some information may be considered an obligation for organisations and a matter of policy. As part of operational preparedness, NGOs should decide what incident information they are willing to share externally, and for what purpose. The table below provides an example of how the sensitivity of information may affect access at all stages of security incident information management, from the location of the incident to a more strategic level within an organisation, as well as between organisations.

Classification	Access
Confidential: Confidential information has significant value for the organisation, and unauthorised disclosure or dissemination of it could result in severe reputational damage or adverse impact on the organisation's operations.	Only those who definitely need access explicitly should be granted it, and only to the least degree necessary (the 'need to know' and 'least privilege' principles). When held outside the organisation's offices such as on laptops, tablets or phones, confidential information should be protected behind dedicated logons and possibly encryption devices and/or encrypted email platforms. This is particularly the case with sensitive cases, such as sexual violence. In such circumstances, any sharing of information needs the explicit informed consent of the affected individual.
Restricted: Disclosure or dissemination of this information is not intended, as it may impact people's lives, cause some negative publicity or limited reputational damage or potential financial losses to the organisation.	Restricted information is subject to controls on access for a small group of staff. Should be held in such a manner that prevents unauthorised access, i.e. on a system that requires a valid and appropriate user to log in before access is granted.
Internal Use: The dissemination of the information to the relevant stakeholders ensures good organisational functioning and internal responses within the organisation. Its release will not cause any damage to the organisation or its staff, but is nonetheless considered undesirable.	Internal use information can be disclosed or disseminated to appropriate members of the organisation, partners and other individuals, as deemed appropriate by the information owners, without any restrictions on content or time of publication.
Public: The dissemination of the information through the news, media and other channels would not pose any risk to the organisation or its staff, and its release is considered desirable or non-objectionable at least.	Public information can be disclosed or disseminated without any restrictions on content. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules.

When deciding on which category information falls into, consideration should also be given to the impact that 'not knowing' will have on other stakeholders.

For example, an abduction incident occurs along a road which is used frequently by many NGOs operating in the area. This may be considered confidential information, as the dissemination of details about this incident could have serious impact on the welfare of staff, the ability to implement programmes and the reputation of the organisation. However, not disseminating the information in a timely manner could lead to others being abducted. Therefore, knowing how information can safely be shared horizontally between actors is important to enable portions of the incident information to be restricted rather than confidential.

Some information should never be publicly disclosed or shared through information sharing mechanism, such as any personal data of individuals affected by an incident, including family contacts, etc.

Incident information sharing and social media

In recent years, social media has become a relevant and significant resource when it comes to obtaining or sharing security-related information. Through the search engines of Twitter or Facebook an enormous amount of contextual and security information can be found.

Social media, including Twitter and Facebook, can also be used to alert others, including groups, about incidents or dangerous situations in a private manner. These information sources, however, need to be understood and managed to ensure secure information management. The recommendations below can be shared with all staff within the organisation and apply at every stage of the SIIM cycle.

Recommendations around social media and incident reporting:

- **Personalise privacy settings:** adjust the privacy settings on the site and select options that limit who can view the information.
- **Separate personal and professional:** use different usernames and photos on different sites, as these can be used to search connections between professional and personal information.
- **Pause before posting:** once something is posted online, it is there forever. Even content that is deleted can sometimes be accessed by the website or through screenshots of the original post. Content that contains personal information, behaviour or whereabouts could pose a security risk.
- **Turn off geolocation:** many social media sites or apps will request access to the device's location, but in most cases this is not necessary. In addition to accessing the device's location, some sites make this information public. When individuals 'check in' on sites like Facebook, they may be sharing their exact location with others.

Because of the nature of the platforms and the speed at which information is shared over social media, information is unverified and may be unreliable. Organisations should consider the source and reliability of information relating to security, and the confidentially of it, before any decision-making or sharing takes place.

"A WhatsApp group that is created for the purpose of informing every SFP from a region of incidents occurring in their area of responsibility should be carefully managed. Only the administrator should be able to add members to the group. Any addition should be validated and at least communicated to all members. Communication rules and codes should be agreed upon and participants should ensure that access to this WhatsApp conversation is protected, should their phone be lost or stolen."

3.2 External sharing of incident information

Sharing with other organisations

Sharing security information, incident and situation reporting, and surveying vulnerabilities between agencies does not come naturally.[22] However, it is increasingly recognised that sharing security information within a specific operational context and rapid reporting of incidents to other NGOs in the area is a collective responsibility.[23]

Organisations can share information directly with each other, through forums or through NGO security information sharing facilities (see 'Forums for sharing security incident information' and 'External contextual trend analysis resources' below).

There are unfortunately many potential barriers to security information sharing between agencies:

- Data pooling for insight into unique NGO security incident patterns requires organisations to be willing to share their aggregate security incident data based on confidentiality agreements.
- Organisational structure, mission, culture, clan, regional, religious, historic, and ethnic misconceptions may obstruct collaboration and sharing of relevant security information.
- Some organisations (or individuals within an organisation) may perceive security as a hindrance to operations while others might place too much emphasis on their autonomy, not associating or collaborating with other stakeholders in the region.
- A clash of personalities between key actors in security matters can severely hinder cooperation and collaboration. While the importance of inter-personal relationships for establishing trust cannot be overstated, formal networks provide a basis to build more formal information sharing structures that are not solely dependent on personality so they will survive staff changes.

[22] Schafer, J. and Murphy, P. (2010). *Security Collaboration: Best Practices Guide*. InterAction Security Unit – InterAction.

[23] Van Brabant, K. (2010). *GPR8 – Operational Security Management in Violent Environments, Revised Edition.* Humanitarian Practice Network/Overseas Development Institute (ODI).

- A general lack of human and financial resources for security often hampers agencies from contributing to or fully participating in collaborative efforts.
- The approach to security can be substantially different between agencies. These differences can make collaboration on common security services difficult, however coordination and sharing of information and approaches will help all parties understand the context better and implement more informed and effective security risk management measures.
- Concerns about indiscreet use of sensitive information shared in coordination mechanisms can often be a substantial barrier to sharing information. There are some examples of information shared in such forums turning up in the press, although this is the exception. It is important to be fully informed of the exact nature of any coordination mechanism, the way information is treated, the expectations and responsibilities for information handling and the consequences of any breach of the terms of the agreement.
- Security is only one of many priorities organisations have when delivering programmes. However, it has been shown time and again that poor security practices and lack of coordination on the part of one organisation can impact the ability of the entire community to gain and retain access for humanitarian and development operations.

Once barriers to sharing information are identified, collaborators should rely on their professionalism and values to find common ground and work towards a mutually agreed solution.

It is important to remember that the behaviour of one organisation can have an impact on the security of all. If an organisation does not relay important incident information, including near misses, it may result in another organisation suffering a high impact event, rather than being able to avoid or minimise the impact of that threat. Collaboration is key for contextual knowledge and overall organisational security.

Sharing with donors

Some organisations send post-incident analysis reports to donors to accompany quarterly or mid-term reports if there has been a break in programming as a result of increasing insecurity or a greater number of incidents. The reports help inform donors about the situation on the ground and aid decisions on programme extension. The organisation should strategically decide whether they wish to share their incident reports with donors, while ensuring they comply with any contractual requirements.

3.3 Forums for sharing security incident information

Below are details of some of the forums and groups dedicated to security coordination and collaboration that specialise in collecting, analysing and sharing security incident information.

Each has a different mandate and therefore different mechanisms for collecting and sharing information. However, all are excellent sources of information and can assist with improving security risk management.

- **Global incident database platforms**
  - Aid Worker Security Database
  - Security in Numbers Database (SiND)
- **Headquarters level**
  - European Interagency Security Forum (EISF)
  - InterAction (United States)
  - Dutch Security Network
  - UK NGO Security Focal Point Group
  - CINFO: Security Community of Practice (Switzerland)
  - Coordinadora Security Working Group (Spain)
  - Canadian Interagency Security Forum
- **Regional level**
  - MENA Region Humanitarian Safety & Security Forum
  - West Africa Regional Security Forum
- **Country level**
  - International NGO Safety Organisation (INSO) and its regional offices
  - Pakistan Humanitarian Forum
  - NGO Forum - South Sudan
- **Others**
  - Security cell meetings with UN agencies, under the Saving Lives Together (SLT) Framework

Some of the information provided by these forums will be public (open source) while others may require membership. Organisations should approach global, regional, local and/or field level forums regarding security-related coordination and information sharing as necessary and where available.

3.4 External contextual trend analysis resources

"NGOs might find it useful to compare their incident trends against that of similar organisations. Such an approach requires sharing of key trend data between organisations in an anonymised format that no longer allows identification of a single agency."

Security managers and analysts should consider analysis of internal incident information as well as security information collected externally, particularly through information-sharing networks.

External incident information allows for stronger contextual knowledge of the NGO's operating environment.

The use of standard classifications makes it easier to compare information between organisations. Standard classifications are provided by the Aid in Danger Project.

See Tool 2: Typology of incidents

The table below gives snapshots of four key resources that provide security incident data and/or trends based on security incident information obtained from multiple sources. It is followed by more detailed information about each resource.

Name	Key features
Aid Worker Security Database (AWSD), run by Humanitarian Outcomes	Provides descriptions of incidents in which staff were killed, injured or kidnapped. An annual report offers insights and analysis of worldwide trends.
Security in Numbers Database (SiND), part of the Aid in Danger project (AiD) by Insecurity Insight	Provides a monthly newsletter of open source events; trend overviews covering a wide range of incidents (beyond those in which staff have been killed, injured or kidnapped); and an analysis of security incidents shared and pooled by agencies. Also provides access to data via Humanitarian Data Exchange.
International NGO Safety Organisation (INSO)	Provides incident information to its member organisations in the countries where it is present. INSO also provides a dashboard showing key incident data.
Saving Lives Together Framework	The Saving Lives Together (SLT) Framework is a joint initiative between the United Nations, international organisations and NGOs. Partner organisations of the SLT receive a variety of incident reports from the United Nations Department of Safety and Security (UNDSS).

Aid Worker Security Database

The Aid Worker Security Database (AWSD), a project of Humanitarian Outcomes, records major incidents of violence against aid workers, with incident reports from 1997 through to the present. Initiated in 2005, the AWSD serves as the sole comprehensive global resource for statistics on major attacks against civilian aid operations, and provides the evidence base for analysis of the changing security environment for humanitarian response.

Incident data is collected from public sources, through systematic media/social media filtering, and from information provided directly to the project by aid organisations and operational security entities. The project also maintains agreements with a number of regional and field-level security consortia for direct information sharing and verification of incidents. Incident reports are cross-checked and verified annually with all relevant humanitarian organisations on an ongoing basis. This includes the United Nations, NGOs and international NGOs in addition to in-country security consortia.

Currently in its fifth year online, the AWSD is the only publicly accessible, interactive database of its kind. The AWSD allows organisations to download the entire dataset and offers an API for external development of applications utilising AWSD data.

The annual Aid Worker Security Report is based on empirical evidence from the data and offers insights and analysis on worldwide trends and recommendations on crucial operational security issues.

For more information or to contribute information and changes to the AWSD, please send an email to info@humanitarianoutcomes.org.

Aid in Danger Project

The Aid in Danger Project by Insecurity Insight systematically monitors open source reports for incidents that negatively affect the delivery of aid and works with aid agency partners to collect and combine their security incident reports. All data are stored in the Security in Numbers Database (SiND) for analysis. The project started in 2008 as a spin-off from the ICRC's Health Care in Danger initiative. Aid in Danger seeks to provide monitoring of the impact of violence and deliberate acts that interfere with the delivery of aid. The Aid in Danger Project tracks a range of incidents that affect the delivery of aid: from threats of violence to administrative decisions to deny permits or visas, to the destruction of infrastructure, and the impact of crime. The project also monitors kidnappings, deaths and injuries of staff.

To respect the confidentiality concerns of participating agencies, the Security in Numbers Database is not publicly available. Datasets containing selected subsets of data, from which personally identifiable information has been removed, are available through Insecurity Insight's page on the Humanitarian Data Exchange.

The Aid in Danger project publicly releases a monthly briefing of open source-reported events, regular updates of trend analyses, and an overview of the confidential agency data in cooperation with the European Interagency Security Forum (EISF).

For more information to become a participating agency, please send an email to info@insecurityinsight.org.

International NGO Safety Organisation

The International NGO Safety Organisation (INSO) is the primary security coordination mechanism for NGOs operating in high-risk contexts, with more than 850 organisational INSO members worldwide.

Founded in 2011, the British charity works on the ground to provide registered NGOs with a range of free services including real-time incident tracking, analytical reports, safety related data and mapping, support for critical incidents and crisis management, policy and site reviews, staff orientations and training on personal safety, security management, and crisis management.

INSO platforms are currently active in Afghanistan, Iraq, Syria, Palestine (Gaza), Somalia, Kenya, DRC, CAR, Cameroon, Nigeria, Mali and Ukraine, with new ones opening annually.

Registration with INSO is strictly limited to local and international NGOs and must be applied for in the country of operation. INSO platforms operate a strict code of conduct in which members share information with one another confidentially.

At the global level, INSO provides timely and accurate NGO security incident data through its Key Data Dashboard and will be launching the Conflict & Humanitarian Data Centre (CHDC) – a centralised database containing all the incidents collected across its network of field platforms – in early 2018.

With more than a million initial entries, the CHDC will be one of the largest global repositories of its type and will support long range, cross-contextual research as well as more immediate tactical analysis.

Eligible NGOs that are not already registered are invited to contact INSO via their registration page or through info@ngosafety.org.

"In some countries, security incidents can be viewed in relation to the events reported by INSO. On a global level, agencies can consult the Aid Worker Security Database for critical events of staff kidnapping, injury or death. For a wider range of incidents, organisations can join the Aid in Danger – Security in Numbers Database."

Saving Lives Together Framework

The Saving Lives Together (SLT) Framework is a joint initiative between the United Nations, international organisations (IOs) and NGOs. Initiated in 2006 and revised in 2015, the SLT framework recognises that the UN and its partner organisations – IOs and NGOs – collectively experience security threats and highlights the importance of collaboration 'to ensure the safe delivery of humanitarian and development assistance'. The objective of SLT is 'to enhance the ability of partner organisations to make informed decisions and implement effective security arrangements to improve the safety and security of personnel and operations'.[24] Partner organisations of the SLT framework receive daily incident reports from UNDSS.

The SLT recommendations, while looking mainly at the collaboration between the UN and international NGOs, provide interesting guidance for organisations to reinforce collaboration in incident information management.[25]

The SLT framework and guidance notes can be downloaded here.

For more information contact UNDSS in country or at a global level via:

Mr Lloyd Cederstrand, OCHA (Operational Liaison and Coordination): cederstrand@un.org

UNDSS Communications Centre (24/7 Emergency Communications Assistance): undsscomscen@un.org, Tel: +1 917 367 9438/9

EISF Executive Director: eisf-director@eisf.eu.

[24] Inter-Agency Standing Committee (IASC). (2015). 'Saving Lives Together – A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field, (October 2015)', *IASC*.

[25] The SLT initiative does not mean that the UN takes responsibility for the security of the whole of the humanitarian community. The UN may have resources such as aircraft for evacuations and communication equipment which they will use, when they can, to support the NGO community, but this is not an obligation, and any costs incurred are likely to be passed to the NGO. NGOs must take responsibility for their own safety and security and resource it appropriately. The same applies for incident information management.

4. OBJECTIVE FOUR: STRATEGIC DECISION-MAKING

This section discusses security incident information management in the context of strategic decision-making, mainly at regional or HQ levels. The intention is to help security focal points and analysts to record security incident information in a systematic manner, to use the information from trend analyses and to communicate findings to key stakeholders within and outside of the organisation. The aim is to inform strategic decision-makers to ensure that the incident information is taken into account at all levels of organisational planning, procedures and projects.This section covers:

- 4.1 Systemic recording of incidents: what system to use?
- 4.2 Analysis of trends to inform strategic decision-making
- 4.3 Organisational structures to discuss strategic security issues
- 4.4 How to use incident information on sexual violence at a strategic level
- 4.5 Using security incident information for strategic advocacy

Relevant tools:

- Tool 2: Typology of incidents
- 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-related decision

The fourth primary objective of security incident information management is to inform strategic decision-making within an organisation.

Regular analysis at HQ level should be carried out to identify trends and patterns to inform strategic long-term decision-making for the entire organisation. The purpose is to take stock of the changing nature of security incidents, to understand the most challenging working environments and the organisation's overall exposure to risk, and to identify the best strategic responses.

A global perspective has become more important with the improvements in communication technology and the availability of information around the world. Incidents can no longer be seen as a purely country-specific issue. For example, an organisational campaign in one region may result in demonstrations at an office on the other side of the world.

Analysis of incident information has implications for good management at a larger scale, which can include decisions around:

- where to operate;
- how to communicate about programmes;
- what insurance policies are needed;
- to what extent security risk management is to be budgeted for within country operations.

Security analysis can also be used to highlight broader concerns about an organisation's core mandate and difficulties in accessing beneficiary populations.

Some organisations carry out this type of analysis on an annual basis, others more frequently. As well as pre-planned reviews, ad-hoc reviews should be carried out whenever there is a significant change in the organisation's mission, profile or operational contexts. Every NGO benefits from regularly discussing their security incident profile. This analysis is made possible through effective information flow between field offices and headquarters and an efficient and effective system that records reported incidents in a systematic and standardised manner to facilitate comparative analysis and strategic decision-making.

Strategic decision-making in relation to security incident information should consider analysis of internal incident information as well as security information collected externally, particularly through information-sharing networks. Comparing internal trends with external ones can flag key internal vulnerabilities and elements of security risk management that require addressing within the organisation.

4.1 Systematic recording of incidents: what system to use?

A good system to record, store, classify and retrieve security incident data is an essential part of security incident analysis and strategic decision-making. Organisations have different mechanisms in place to report, collect and record country level incidents in a central location. In relation to online systems, there are numerous solutions that range from free, open source, easily self-customisable models to tailor-made systems prepared by commercial corporations.

Whatever system an organisation uses, it is important that the incident recording and mapping system is designed to respond to the needs of all the users, from reporting to trend analysis. New technologies can help with this.

There are two approaches an NGO can take in using technology to develop an incident recording and mapping system:

- a stand-alone solution integrated into the servers and systems of the organisation; or
- 'software as a service' where the system is hosted by an external service provider.

The decision on what approach to take will depend on factors such as the technological strategy and size of the organisation, the likely number of incidents, resources and capacity to manage the system, and data protection. The following table is a summary of some of the available systems to report, store and analyse security incidents that affected an organisation at a central level.

	Incident reporting and recording method	System
In-house Designed and Managed System	Written narrative of the incident; associated with a spreadsheet to record incidents using systematic coding	This could be through e-mails, Google docs or sheets, a shared Google platform, SharePoint. A spreadsheet can be used to classify information submitted in a written format by using specific data fields that have to be completed.
	Online system utilising existing open source platforms	The incident reporting system can be built as an extension to existing platforms used for email, such as SharePoint. Online geo-based platforms such as Ushahidi can be customised to create a global incident reporting and information management system.
External Systems	Subscription to an online platform for data management	Some private companies and non-profit organisations offer online platforms for security incident information management.
	Custom-built online system	Some organisations have commissioned the development of organisation-specific online systems.

See Tool 9: SIIM systems for a more detailed table that illustrates the available systems for incident information management and a summary of disadvantages and advantages of these different systems.

Smaller organisations or NGOs with limited resources may opt for the first two methods of incident recording and reporting given the simple set up and maintenance of these systems, as well as their relative low cost. The more advanced systems may suit larger organisations which experience a high number of incidents and require a flexible system that corresponds to the specific needs of the organisation.[26]

Incident storing tools

A basic incident storing template should contain the following information:

- **Country, region and location** – be specific.
- **Date and time of the day** – when the incident happened, how long it lasted and when the incident was closed.
- **What happened** – a brief and concise synopsis of the incident.
- **Category of incident** - Analytical categories for data trend analysis – see Tools 2 and 10 for suggested options.
- **Who was involved** – both internal and external, both victims and management support.
- **Actions and decisions taken** – summary of key actions/ decisions taken and by whom.
- **Operational changes** – overview of immediate changes made in reaction to the incident.
- **Analysis and comments** – summary of the analysis document following the incident.
- **Status** – is the security incident ongoing? Has all the information been documented?

This handbook provides examples of incident storing tools in Excel. These documents can be found under Tool 2: Typology of Incident and Tool 10: Incident storing.

Future analysis and statistics needs should be identified before the incident storing tool is designed; columns should be created to enable trend analysis and statistics development using Excel settings.

Online systems

Key functions an organisation may look for in an online system:

- A single web-based repository of incidents;
- Provides electronic reporting from internet connected PC or mobile device;
- Notifies different groups based upon details in the submitted incident report;
- Ensures data security – submitted information is accessible only on a controlled, need-to-know basis;
- Ensures data is protected in transit;
- Ensures data is backed up.

[26] De Palacios, G. (2017, forthcoming). 'Managing security-related information: a closer look at incident reporting systems', *EISF*.

Key things to decide upon:

- How end users will feed into the repository;
- How to ensure that access to the repository is secured on a need-to-know basis;
- How to notify different groups of people based upon details in the incident submission;
- How to ensure that information is completely and accurately captured from the incident source;
- How to validate the captured information electronically;
- To what extent the system would be used for case follow-up (would it be just a repository or would there also be follow-up stages?);
- What kind of analysis functions to build on top.

Key things to have in place before embarking on the development of an online system:

- Definition of categories of incidents;
- Clear instructions for users about the categories.

No matter what the tools and systems, it is important to define, technically, who accesses the stored data at field, national, regional and HQ level. Passwords, encryptions, closed group, peer validation processes for access, etc., are examples of methods that can be used to ensure information is shared with the appropriate stakeholders. See 'Introduction – Information security' for more details on information security.

See Tool 11: Technology to report and record incidents for examples and descriptions of online systems to record and report incidents.

4.2 Analysis of trends to inform strategic decision-making

Once the incident information is consolidated in one central system and includes analytical categories it is possible to more strategically analyse security information to inform decisions.

Security managers, focal points and analysts should transform data into useful information. This information will be shared with identified senior staff in the form of trends and statistics to support decision-making processes.

Most organisations classify security and safety incidents. Categorising helps with analysis and extracting statistics.

Data can be broken down by key categories (Tool 2: Typology of incidents) and presented in the form of trend analysis overview reports (Tool 12: Analysing data trends).

The nature of this strategic-level analysis depends on the number of security incidents reported within an organisation. If there are only a handful, a written note that summarises key events can be the best method of presenting trends. If the number of reported events increases, it will be important to develop more systematic figure-based trend monitoring.

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.

- What kind of security incidents did staff and the organisation experience?
- In which countries did they occur?
- As HQ security focal point how satisfied are you with the way country offices appear to have used security incidents, including near misses, to learn and improve their practices?
- What security incidents are other organisations experiencing in the same country and how does this compare to the incidents reported within your organisation?
- How did the security incidents affect the delivery of aid?
- Can we cost the impact of security incidents on the delivery of aid?
- What were the main causes of security incidents?
- Can the causes of incidents be classified in terms of the response strategy that may be needed?
- Can we use the data to identify a risk threshold our organisation is prepared to accept?

See Tool 13: Strategic-level questions for incident information management-related decisions for a complete list of questions and possible recommended actions.

Google Earth Pro Visualisation Tool

Geographic mapping of events can be a useful tool to visualise incidents to support analysis and reporting to senior management within the organisation. Multiple options exist to display information visually. If this is the preferred option, the necessary details for geolocation and incident type must be included as part of the initial report, as it is not effective or accurate to do this retrospectively.

If the right information is available (e.g. GPS coordinates, colour codes, incident types, etc.), a simple option to show the location of incidents can be to convert an Excel document into a KML document and then to link this to Google Earth Pro. If the Excel-KML document contains the proper information, then events will be pin-pointed automatically on a Google map.[27]

Make sure your settings ensure confidentiality by reducing access to the information.

4.3 Organisational structures to discuss strategic security issues

Organisations can discuss security issues from a strategic perspective in multiple settings.

A security risk management committee, for example, may meet at regular intervals (e.g. once a year or more frequently) to bring together appointed board members, the CEO, the security focal point or security team, and possibly regional directors. Security personnel are often tasked with preparing the meeting, at which they then present security trends and elaborate the agenda for discussion.

[27] For step by step guidance on the process of converting an Excel document to KML see: https://www.earthpoint.us/ExcelToKml.aspx

In this type of meeting, it may be beneficial to cover:

- Security incident trends over the past years, presented as:
  - a table of security incidents per country;
  - a table of security incidents per category;
  - a table on seriousness of incidents (i.e. impact);
  - a table on causes of incidents;
- An analysis of the consequences of reported security incidents, for example:
  - human consequences with psychological and/or physical impact;
  - operational consequences;
  - organisational consequences such as those affecting the NGO's reputation,
  - consequences for security risk management;
- Recommendations on how to ensure work continues in these environments.
- Context ratings and operational security levels.
- Obstacles to incident reporting in the organisation.
- A case study that illustrates an important theme to be discussed with everyone and that leads to the development of an action plan for future similar cases (e.g. communications plan in case of incidents, whether to establish relation ships with local authorities, etc.).
- Space for addressing questions from the decision-makers present to the security personnel.

For more examples of how to prepare security analysis for review meetings see Tool 12: Analysing data trends.

The review of security documents, such as organisational security risk threshold, security risk management framework, security strategy, security policy, the crisis management plan, etc., should be included as an agenda item for every meeting even if the action point is 'no action required'. This is important for documenting due process for duty of care.

4.4 How to use incident information on sexual violence at a strategic level

The best way for organisations to approach incidents of sexual violence against their staff is to learn from the experience to ensure that the organisation does a better job of protecting its staff and responding to these types of incidents in the future. This continues to be a topic people find difficult to discuss so the organisation should actively endeavour to create trust and openness to discuss these incidents internally.

Analysis should be conducted as to whether it would be strategic and beneficial to be open about incidents of sexual violence with media outlets or within global forums with other members of the NGO community.

"Being open on a larger platform can also create the space for other NGOs to undertake similar change within their own organisations, contributing to an overall increase in the safety and security of NGO staff."

If details about a specific event are to be used to highlight the issue and lessons learned at the global level, the survivor must give their informed consent. Where possible the survivor should be engaged in this process and provide a guiding voice to the creation of a narrative around the incident and the lessons learned.

Where the survivor has given informed consent for information about their experience to be shared – at the field or global level – ensure that they are provided with additional support around the time when the information is made public, including compassionate leave, psychosocial support, etc.

It is possible to share trend information and organisational learnings without compromising the individual's rights and this should be encouraged.

4.5 Using security incident information for strategic advocacy

An organisation should decide, strategically, whether to use incident information obtained internally, and potentially also externally, for the purposes of advocacy.

Many organisations report a growing difficulty in securing the safe passage and delivery of aid to civilians in need. However, without sector-wide consolidated data about such incidents and in the absence of an effective collective strategy on how to address deliberate obstructions or impunity for perpetrators, most agencies can only bring up individual cases by themselves.

NGOs have made great progress in developing security risk management strategies to respond to ever-changing security contexts. However, this has not been matched by a common humanitarian advocacy to address concerns that are beyond an individual organisation's security risk management strategy. The scale of insecurity for humanitarian action thus remains hidden, each case being dealt with in silence and, in most cases, with perpetrators rarely brought to justice. There are opportunities to develop a sector-wide advocacy strategy to address complex concerns.

Some security incidents are beyond what an organisation can control and may require a joint advocacy campaign with other organisations. For example, the increasing use of explosive weapons in populated areas affects the security of staff and hinders the delivery of aid. When national authorities do not take required measures against perpetrators, organisations may need to seek international support with investigations or to pressure for prosecutions.

At a more global level, it is important for the aid sector to ensure that information on the challenges created by volatile security contexts is regularly made available to key stakeholders such as donors, policy-makers, the media and the general public. Documented evidence of violence against aid workers or incidents that affect the delivery of aid are needed to support broader efforts to improve the protection of aid workers and their operations to support unhindered access to populations in need. Collectively, the humanitarian and development sector could do more to remind the donating public and policy-makers of the difficulties and dangers aid workers face when delivering aid in insecure environments.

However, when organisations are considering whether to carry out an advocacy campaign, they must consider possible consequences for staff safety and security as well as programme implementation.

What kind of data is needed for advocacy?

There is a tendency in the media and among other stakeholders to ask first for figures that illustrate the scale of the problem. Consequently, much effort has been put into trying to quantify how many people are affected. However, this is not necessarily needed for a policy discussion. Past campaigns have shown that the description of the nature of a problem can be powerful enough to encourage change. The anti-personnel landmine campaign, for example, started with a focus on the presentation of individual contexts with details from the International Committee of the Red Cross (ICRC) programmes in Cambodia and Angola that illustrated, rather than quantified, a problem. As the vivid description of the impact of landmines on the individual spoke to many, the campaign was able to achieve impressive results.[28]

Incidents affecting NGO security can be used to describe the nature and the impact of a problem even when it is not known how frequent it is. There are opportunities for the aid community to reach out to a wider public and key policy-makers with strong narratives of how their work and staff are affected by the contexts they work in.

One of the most convincing sources demonstrating the impact of insecurity on the delivery of aid are the incident reports organisations generate for their own security risk management. The mere existence of the data demonstrates the problem better than any data specifically collected for advocacy purposes. It may be a missed opportunity not to tap into this resource to make the case for better protection or, at least, better funding for security-related policies and improved security training for staff.

Generating this data collectively as a sector can contribute to stronger advocacy for the protection of aid workers and programmes, and greater acceptance by donors that security risk management is a direct cost that should be included in proposals.

It is important not to expose individuals or specific cases for the purposes of making a political point. Collective data reduces this risk.

Senior management within organisations can advance this agenda by contributing to data sharing with other organisations and by strengthening links between security personnel and policy and advocacy staff within their own organisation. This helps ensure that the insight from multi-organisational security incident analyses is used by policy and advocacy staff strategically.

[28] For a general description of the elements that made the 'ban landmines' campaign so effective see the following article here. One of the first and highly influential articles by the ICRC acknowledged that the total figure was not known but described the impact and the effect of landmines in general terms on civilians. See the article here.

Case study: Health Care in Danger, ICRC

In 2008, the ICRC commissioned a study across 16 countries to document how violence affected the delivery of health care, using incident data from selected contexts.[29] This study became the first evidence base to start addressing violence against health care workers, which has since been illustrated by numerous additional case studies.[30] Since then, the ICRC has run the Health Care in Danger project, which combines awareness-raising with practical guidance on how to improve the security of health care workers.[31]

Other organisations have also started to take up this issue. Since 2014, ten members of the Safeguarding Health in Conflict Coalition have jointly published annual reports on attacks on health care, which combine data and information from different organisations to keep the issue on the global agenda.[32] More than 20 members of the coalition, including several humanitarian organisations, help to disseminate the information to encourage better protection of health care.[33]

In 2016, the World Health Organisation (WHO) published data relating to attacks on health care on its website.[34]

In May 2016, the UN Security Council adopted Resolution 2286 which set out a roadmap for the protection of health care in conflict.[35]

These examples highlight how the effective use of data can help to put, and keep, this important issue on the agenda.

The Working Group for the Protection of Humanitarian Action

The Working Group for the Protection of Humanitarian Action is considering options for collective global action to protect aid workers.[36] The working group brings together practitioners from operational humanitarian organisations, security experts, advocacy and policy experts and academics, and is jointly led by the Advanced Training Programme on Humanitarian Action at the Harvard Humanitarian Initiative, and Action Against Hunger/Action contre la Faim. The aim is to overcome the tendency of humanitarian organisations to work in isolation respond to this increasingly challenging environment through collective reflection, stronger and more consistent advocacy across the humanitarian sector, and joint actions to reassert respect for international humanitarian law (IHL) and the protection of humanitarian action. IHL being the responsibility of states, it is only on the global scale that the humanitarian community can push for a change in a context that is, for now, becoming less conducive for humanitarian aid to reach civilians in need.

29 ICRC. (2011). *A sixteen-country study: health care in danger.* ICRC.
30 For more information see: http://healthcareindanger.org/resource-centre/
31 For more information see: http://healthcareindanger.org/hcid-project/
32 For more information see: https://www.safeguardinghealth.org/
33 For a list of humanitarian organisations that support the Safeguarding Health in Conflict Coalition see page 2 here.
34 See: http://www.who.int/emergencies/attacks-on-health-care/en/. Please note that this site will soon be upgraded. See also Lieberman, A. (2017). 'WHO readies to launch online database tracking health worker attacks', *Devex*.
35 United Nations. (2016). 'Security Council Adopts Resolution 2286 (2016), Strongly Condemning Attacks against Medical Facilities, Personnel in Conflict Situations', *United Nations*.
36 ATHA. (2016). 'Policy Project: Protection of Humanitarian Action', *ATHA*.

One of the initial findings of the working group was that better systematic information sharing on security incidents is required in order to help identify key trends and priorities. The working group also identified a lack of direct cooperation and communication between security risk managers and advocacy departments in many organisations as an obstacle to more effective work. The working group seeks to engage with security focal points and policy staff within organisations to identify cases where common advocacy can support the response to security concerns.

For more information on the working group please contact:
Lise Fouquat: lfouquat@actioncontrelafaim.org
Pauline Chetcuti: pchetcuti@actioncontrelafaim.org
Julia Brooks: jbrooks@hsph.harvard.edu

CHAPTER 3: TOOLS

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:

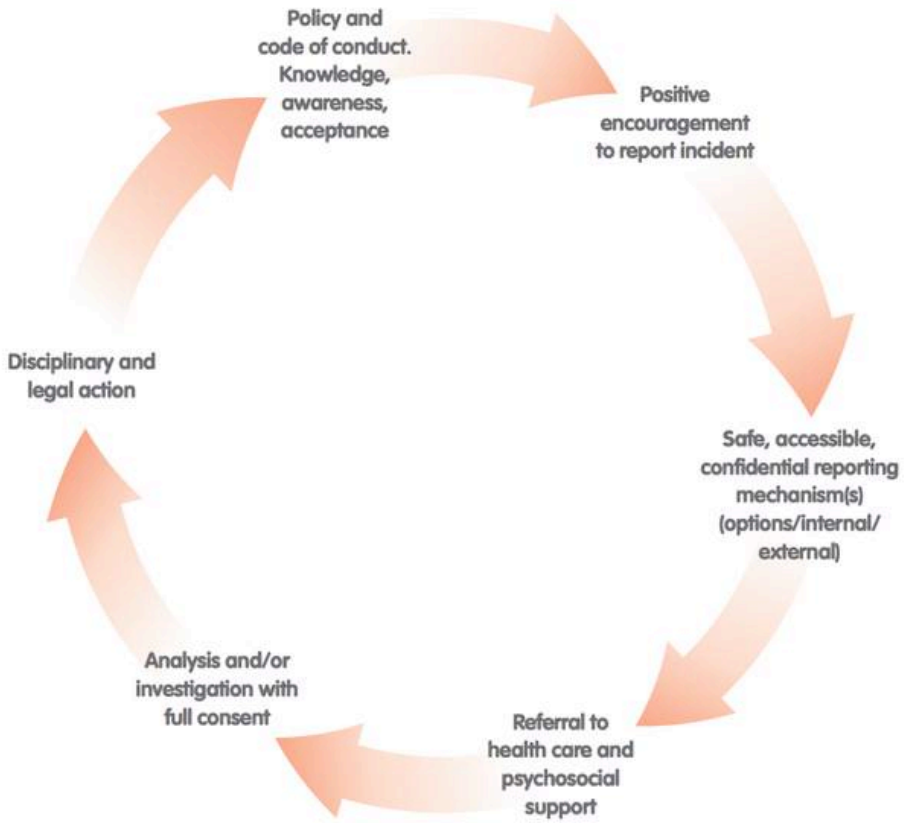
- Was a hazardous condition a contributing factor?
- Was the location a contributing factor?
- Was the procedure a contributing factor?
- Was lack of personal protective equipment or emergency equipment a contributing factor?
- Were the SOPs a contributing factor, and should they be updated to reflect 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

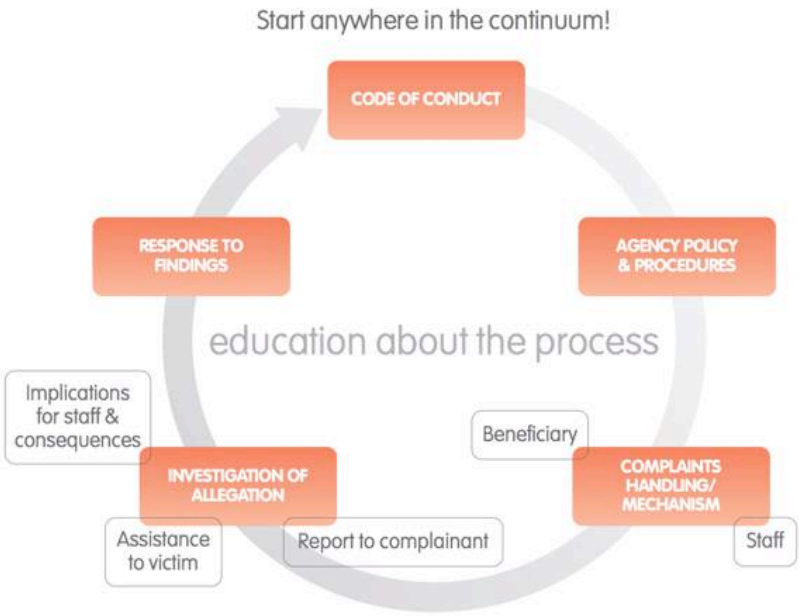
laws governing employers and employees permit, coordinate with other agencies to establish a system for sharing information about employees whose contracts have been terminated for engaging in harassment, sexual violence and/or SEA. Careful hiring practices that include reference checks and vetting are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

REFERENCES AND BIBLIOGRAPHY

ATHA. (2016). 'Policy Project: Protection of Humanitarian Action', *ATHA*. Available from: http://www.atha.se/policy-project-protection-of-aid-workers

Ayre, R. (2010). *The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field*. EISF. Available from: https://www.eisf.eu/wp-content/uploads/2014/09/0119-Ayre-EISF-2010-The-Information-Management-Challenge-A-Briefing-on-Information-Security-for-Humanitarian-Non-Governmental-Organisations-in-the-Field.pdf

Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs*. EISF. Available from: https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/

Buth, P. (2010). *Crisis management of critical incidents*. EISF. Available from: https://www.eisf.eu/wp-content/uploads/2014/09/0121-Buth-2010-Crisis-Management-of-Critical-incident-2010.pdf

Davidson, S. (2013). *Managing the message: Communication and media management in a security crisis*. EISF. Available from: https://www.eisf.eu/wp-content/uploads/2014/09/1140-Davidson-2013-Managing-the-Message-Communication-and-media-management-in-a-security-crisis.pdf

Davis, J. et al. (2017). *Security to go: a risk management toolkit for humanitarian aid agencies. 2nd edition*. EISF. Available from: https://www.eisf.eu/wp-content/uploads/2017/03/2124-EISF-2017-Security-to-go_a-risk-management-toolkit-for-humanitarian-aid-agencies-2nd-edition.pdf

De Palacios, G. (2017). Forthcoming publication 'Managing security-related information: a closer look at incident reporting systems', *EISF*.

Dick, A. (2010). *Creating Common NGO Security Terminology: A comparative study*. Security Management Initiative. Available from: https://www.eisf.eu/wp-content/uploads/2014/09/0647-Dick-2010-Creating-Common-NGO-Security-Terminology-A-Comparative-Study.pdf

Earth Point. (unknown). 'Excel To KML - Display Excel files on Google Earth', *Earth Point*. Available from: https://www.earthpoint.us/ExcelToKml.aspx

Hoelscher, K., Miklian, J. and H. M. Nygård. (2015). *Understanding Attacks on Humanitarian Aid Workers*. Peace Research Institute Oslo (PRIO) Conflict Trends. Available from: http://file.prio.no/publication_files/prio/Hoelscher,%20Miklian,%20Nyg%C3%A5rd%20-%20Understanding%20Attacks%20on%20Humanitarian%20Aid%20Workers,%20Conflict%20Trends%206-2015.pdf

ICRC. (2011). *A sixteen-country study: health care in danger*. ICRC. Available from: https://www.icrc.org/eng/assets/files/reports/report-hcid-16-country-study-2011-08-10.pdf?__hstc=163349155.76b9edd98545ef10cf2630f8704dd68b.1500037719517.1500037719517.1500838137193.2&__hssc=163349155.2.1500838137193&__hsfp=520750989

InterAction. (2010). *InterAction Step by Step Guide to Addressing Sexual Exploitation and abuse*. InterAction. Available from: https://www.interaction.org/sites/default/files/2010.6%20-%20Step%20by%20Step%20Guide%20-%20Comments%20Version.pdf

Inter-Agency Standing Committee (IASC). (2008). *Operational guidance on responsibilities of cluster/sector leads & OCHA in information management*. WHO. Available from: http://www.who.int/hac/network/global_health_cluster/iasc_operational_guidance_on_information_management_v3.pdf

Inter-Agency Standing Committee (IASC). (2015). 'Saving Lives Together – A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field, (October 2015)', *IASC*. Available from: https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0

Inter-Agency Standing Committee (IASC). (2015). *Guidelines for Integrating Gender-Based Violence Interventions in Humanitarian Action: Reducing risk, promoting resilience and aiding recovery*. Available from: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/femm/dv/gbv_toolkit_book_01_20_2015_/gbv_toolkit_book_01_20_2015_en.pdf

Inter-Agency Standing Committee (IASC). (2016). *Protection from Sexual Exploitation and Abuse (PSEA) Inter-agency cooperation in community-based complaint mechanisms: Global Standard Operating Procedures*. IASC. Available from: http://reliefweb.int/report/world/protection-sexual-exploitation-and-abuse-psea-inter-agency-cooperation-community-based

International Organization for Standardization (ISO). (2009). ISO 31000:2009: Risk Management – Principles and guidelines.

International Organization for Standardization (ISO). (2014). ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary.

Irish Aid. (2013). *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*. ALNAP. Available from: http://www.alnap.org/resource/11229

Kemp, E. and Merkelbach, M. (2011). 'Can you get sued? Legal liability of international humanitarian aid organisations towards their staff', *Security Management Initiative*. Available from: https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

Kemp, E. and Merkelbach, M. (2016). 'Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications', *EISF*. Available from: https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/

Lieberman, A. (2017). 'WHO readies to launch online database tracking health worker attacks', *Devex*. Available from: https://www.devex.com/news/who-readies-to-launch-online-database-tracking-health-worker-attacks-90331#.WWYjVPrtmqh.twitter

Martinsson, J. (2010). 'Important Lessons from the Landmine Campaign', *The World Bank*. Available from: https://blogs.worldbank.org/publicsphere/important-lessons-landmine-s-campaign%20

Merkelbach, M. (2017). *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel*. Swiss Federal Department of Foreign Affairs (FDFA), Stabilisation Unit (SU) and Center for International Peace Operations (ZIF). Available from: http://www.zif-berlin.org/fileadmin/uploads/experten-einsaetze/Voluntary_Guidelines_on_the_Duty_of_Care_to_Seconded_Civilian_Personnel_Final_170420.pdf

Nobert, M. (2016). *Prevention, Policy and Procedure Checklist: Responding to Sexual Violence in Humanitarian and Development Settings*. Report the Abuse. Available from: http://www.reporttheabuse.org/take-action/preventing-sexual-violence/

Nobert, M. (2017). 'Why should we address sexual violence in humanitarian workplaces?', *EISF*. Available from: https://www.eisf.eu/news/why-should-we-address-sexual-violence-in-humanitarian-workplaces/

Parlov, A. (1995). 'Toward a global ban on landmines', *International Review of the Red Cross*. Available from: https://www.icrc.org/eng/resources/documents/article/other/57jmmj.htm

Persaud, C. (2012). *Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management*. EISF. Available from: https://www.eisf.eu/wp-content/uploads/2014/09/1137-Persaud-2012-Gender-and-Security-Guidelines-for-Mainstreaming-Gender-in-Security-Risk-Management.pdf

RedR UK and EISF. (2016). *Report: Inclusion and security of LGBTI aid workers*. RedR UK. Available from: https://www.eisf.eu/wp-content/uploads/2016/08/2091-RedR-and-EISF-2016-REPORT-INCLUSION-AND-SECURITY-OF-LGBTI-AID-WORKERS-WORKSHOP-22-01-2016.pdf

Safeguarding Health in Conflict Coalition. (2017). *Impunity must end: attacks on health in 23 countries in conflict in 2016*. Available from: https://www.safeguardinghealth.org/sites/shcc/files/SHCC2017final.pdf

Saving Lives Together. (2016). 'Guidelines for the Implementation of the "Saving Lives Together" Framework', *Saving Lives Together*. July 2016. Available from: https://www.eisf.eu/library/guidelines-for-the-implementation-of-the-saving-lives-together-framework/

Schafer, J. and Murphy, P. (2010). *Security Collaboration: Best Practices Guide*. InterAction Security Unit – InterAction. Available from: https://acceptanceresearch.files.wordpress.com/2010/10/interaction_security-collaboration-best-practices-guide-201111.pdf

United Nations. (2016). 'Security Council Adopts Resolution 2286 (2016), Strongly Condemning Attacks against Medical Facilities, Personnel in Conflict Situations', *United Nations*. Available from: https://www.un.org/press/en/2016/sc12347.doc.htm

United States Army. (2006). *Field Manual No. 2-22.3. Human Intelligence Collector Operations*. Available from: https://fas.org/irp/doddir/army/fm2-22-3.pdf

Van Brabant, K. (2001). *HPG Report 9: Mainstreaming the Organisational Management of Safety and Security*. Humanitarian Policy Group/ODI. Available from: https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/297.pdf

Van Brabant, K. (2010). *GPR8 – Operational Security Management in Violent Environments, Revised Edition*. Humanitarian Practice Network/Overseas Development Institute (ODI). Available from: http://odihpn.org/wp-content/uploads/2010/11/GPR_8_revised2.pdf

Wansbrough-Jones, A. and Dixon, M. (2014). *"Saving Lives Together": A Review of existing NGO and United Nations Security Coordination Practices in the Field*. Coordination Toolkit. Available from: http://www.coordinationtoolkit.org/wp-content/uploads/Saving-Lives-Together-Review-of-NGO-and-UN-Security-Coordination-Practices.pdf

WHO, War Trauma Foundation and World Vision International. (2011). *Psychological first aid: Guide for field workers*. WHO. Available from: http://www.who.int/mental_health/publications/guide_field_workers/en/

WHO. (2017). *Attacks on Health Care webpage*. Available from: http://www.who.int/emergencies/attacks-on-health-care/en/

Wille, C. (2016). 'Lessons from the Aviation Industry: What Can We Learn for Humanitarian Security Risk Management?', *EISF*. Available from: https://www.eisf.eu/news/lessons-from-the-aviation-industry-what-can-we-learn-for-humanitarian-security-risk-management/

Williamson, C. (2017). 'People management' in Security to go: a risk management toolkit for humanitarian aid agencies. *EISF*. Available from: https://www.eisf.eu/news/people-management-and-security-risk-management/

ADDITIONAL INFORMATION

ORGANISATIONS

RedR UK is an international humanitarian NGO which supports humanitarian actors across the world through training and technical support. Founded in 1980 as a membership roster, RedR has become a leading agency in building the capacity of the sector reaching tens of thousands of humanitarian professionals and hundreds of organisations. We have an international presence with offices in the UK, Sudan, Kenya and Jordan and provide training to humanitarians globally from these regional hubs.

RedR UK is a leading provider of training and capacity building support to the humanitarian sector, training over 7,000 humanitarians in more than 55 countries each year. Having worked in humanitarian capacity building for over 35 years supporting tens of thousands of humanitarians, RedR has developed expertise that makes us a leader in adult learning within the sector. We have experience of delivering capacity building programmes that include face to face training, coaching and mentoring, desk top and field based simulations, deployments, short-term consultancies and online learning. In addition to our high-quality learning programmes we have made significant contributions to the effectiveness of learning provision in the sector. RedR UK's experience in delivering and managing innovative humanitarian capacity building programmes makes RedR UK well placed to manage the Security Incident Information Management project.

Insecurity Insight is a leading group of experts dedicated to generating and analysing 'data on people in danger', with a track record in developing state of the art incident monitoring systems for the humanitarian community. Since 2009, Insecurity Insight has worked in partnership with humanitarian agencies to develop a mechanism for confidential agency incident sharing and analysis.

European Interagency Security Forum is an independent network of security focal points who currently represent 85 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice. EISF facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

CONTACTS

To share resources and to know more about the project, please contact:

RedR UK	Marine Menier: marine.menier@redr.org.uk
Insecurity Insight	Christina Wille: christina.wille@insecurityinsight.org
EISF	Lisa Reilly: eisf-director@eisf.eu