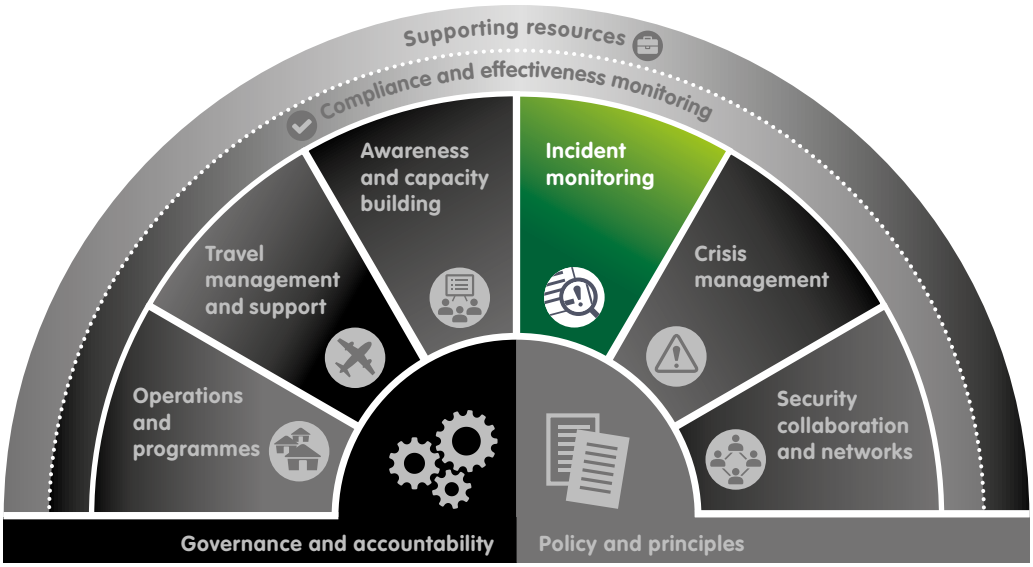
8 Incident monitoring



Timely reporting of incidents is essential to protect your staff. It ensures that staff receive assistance quickly and that the incident response and its aftermath are effectively managed. A good incident monitoring system will help colleagues avoid similar incidents and react appropriately to changes in the operating environment. It will also improve understanding of the context and support management decision-making.

Regular reporting and monitoring of incidents enables organisations to determine where and how the security situation is changing, why it is changing, and what these changes mean for staff security.

For most smaller NGOs, investing in extensive incident reporting systems and software offers little value, as they are likely to have relatively few incidents to deal with. However, establishing a basic system for reporting and recording security incidents is vital for all organisations, large and small. A basic incident monitoring system consists of two key components:

1. A process for initially reporting an incident or situation;
2. A system for handling the reported information.

Incident reporting procedures

Incident reporting procedures should provide clear guidance on which incidents should be reported, to whom, and the mechanism for doing so.

It is not easy to introduce an incident reporting system into an organisation - it takes time and perseverance for it to take hold and for all incidents to get reported. Under-reporting of security incidents is a challenge in all organisations, so you will need to communicate clearly to staff the purpose, justification and expected benefits of reporting incidents. Better awareness of the need for reporting, trust in how the organisation handles the information, feedback to staff when they report incidents, and an easy-to-use mechanism are crucial in establishing an effective reporting system.

What to report

For many organisations, a security incident is: **any situation or event that has caused, or could result in, harm to staff, associated personnel or a third party, significant disruption to programmes and activities, or substantial damage or loss to the organisation's property or its reputation**.

'Near misses' must also be reported as they may prevent others from being involved in an incident and help staff to understand if and how the security context is changing.

While staff must be encouraged to report all incidents, you will need to be very clear about what a reportable incident is. Perceptions of what is an incident will vary greatly between staff members and locations, depending on what is considered the norm in that context. While you can be confident that major incidents will be reported, there is a risk that staff will overlook or dismiss seemingly isolated or insignificant incidents which, when viewed together, may signify a change in their security situation.

'Near miss' incidents must also be reported. A 'near miss' is an occasion when, either through luck or an appropriate response, a serious incident was avoided.

All serious incidents must be fully examined to understand the events leading up to, during and after the incident. A post-incident inquiry, ideally led by someone not connected with the incident, should consider possible motives or causes, the actions and behaviour of staff, and the response to the incident. Incident investigations should identify key recommendations or

follow-on actions, including possible disciplinary procedures, to continually improve security risk management.

Incident reports

As a minimum, reports should address the ***'Five Ws'***: ***Who*** did ***What*** to ***Whom***, ***Where*** and ***When***.

There are typically three types of incident reports:

- **Immediate incident report** – sent the moment the incident occurs or as soon as possible thereafter (when it is safe to do so), normally verbally over the phone or radio, providing a brief summary of what has happened, and any action/support required.
- **Incident updates** – sent as often as necessary, to provide more information on the incident or situation.
- **Post-incident report** – sent after the incident is stabilised or over, providing a written account of the incident and the various actions taken.

Incident report forms

A standardised and easy-to-use incident report form can bring clarity and consistency to your organisation's reporting process. A formal post-incident report should be completed for all security incidents that directly involve your staff or others working on behalf of your organisation. Reports should also be completed following any incident that results in substantial loss or damage to property, or injury or harm to a third party.

A security incident report should provide a complete written account of the incident and the various actions that were taken. A standard template should be created for all post-incident reports.

There will be information that must be treated confidentially, such as certain health conditions, incidents of sexual assault, names of victims, etc. Staff must be provided with guidance on how to handle sensitive or confidential information in order to preserve confidentiality, for example, guidance on who is permitted to access the incident reports, and when and how access to reports should be restricted.

Incident report form

An incident report form should include:

- **Type of incident** – clarifying the type of incident, for example, theft, burglary or armed robbery.
- **Location** – where the incident occurred, using precise locations.
- **Date, day and time** – when the incident occurred as precisely as possible.
- **Who is involved** – who was affected by the incident, including their position, type of programme, nationality, gender, etc., to improve understanding of specific vulnerabilities.
- **Incident description** – a detailed description of the nature of the events, the impact on those affected, and details of any material losses, etc.
- **Incident analysis** – an initial assessment of who may have perpetrated the incident, what caused the incident, whether the organisation or staff were specifically targeted, and the possible implications for the future security of staff.
- **Immediate decisions and actions taken** – information on the decisions and actions taken, and by whom, immediately after the incident.
- **Who has been informed** – a list detailing who the incident has been reported to locally, for example, authorities, other aid agencies, donors or other key stakeholders.
- **Further actions to be taken** – detail the decisions and actions that need to be taken in response to the incident. Give any recommendations for improving staff security.

Further information

Incident Report Template Example

'Chapter 5: Incident reporting and critical incident management' in ODI guide 'GPR8 - Operational Security Management in Violent Environments'

'Guidance Tool F: Good practice in gender-sensitive incident reporting' in EISF briefing paper 'Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management'

Incident logging and analysis

Records of all security incidents should be centralised and analysed periodically. In addition to providing an institutional record of the incident and the organisation's response in the event of litigation or external enquiries, analysing this stored information will allow your organisation to develop a

broader, more global understanding of the security issues affecting your staff.

Regular analysis of your organisation's incident reports can be used to:

- Raise awareness of security among staff and therefore strengthen the organisation's security culture;
- Increase understanding among senior managers, and within the Board of Trustees, as to the organisation's risk profile, the main threats that affect staff, and gaps in procedures, support and training;
- Provide analysis to improve decision-making for programme design and implementation;
- Negotiate with insurance providers. Insurers often rely on 'global statistics' to set premiums, but if you can demonstrate the specific risks your organisation is exposed to and the measures you have in place to manage these, you might persuade them to lower their premiums, or at least not to increase them.

There are now several off-the-shelf software packages and open source software tools that can be utilised to record and analyse incident data, and many organisations have established their own comprehensive incident reporting databases. However, for some NGOs, these may seem either too costly or complex to set up and maintain. You may find that using simple Excel spreadsheets to log key information from different incident reports is more than sufficient for your organisation.

It is advisable to share information between different agencies, where possible, in order for your organisation to benefit from a greater understanding of the context - for example, by accessing and contributing to Insecurity Insight's Aid in Danger project and Humanitarian Outcomes' Aid Worker Security Database.

Further information

'Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study' by Gonzalo de Palacios in the EISF briefing paper 'Communications Technology and Humanitarian Delivery'

EISF briefing paper 'Incident Statistics in Aid Worker Safety and Security Management'

'Managing security information - Simson software' by the Centre for Safety and Development

Aid in Danger Project by Insecurity Insight

Aid Worker Security Database by Humanitarian Outcomes

Incident Dashboard by INSO