SECURITY INCIDENT INFORMATION MANAGEMENT
HANDBOOK
USER GUIDE

Understanding the operational context

Immediate response

Strategic decision-making

Security

Incident

Lesson’s learned and applied

Information

Tools

Organisational security risk management

Data on People in Danger
What is security incident information management?

Security incident information management (SIIM) is the collection, reporting, recording, analysis, sharing and use of information (including data) linked to security incidents. 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.

What is the User Guide?

The SIIM Handbook User Guide is designed to be used in conjunction with the SIIM Handbook. It is a document which enables staff to access the parts of the handbook which are most relevant to them, their position within the organisation and what they want to know. On page three is a list of roles, and on pages four to eleven are the different tasks that those roles might be doing, with details of which sections and tools within the handbook will be most helpful.

Who is the 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 (NGO), 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.

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 guidance and accompanying tools to assess the security incident information management needs of their organisation.
- Use the tools provided in the handbook to improve their organisation’s security incident information management system.

The handbook can be consulted as a whole, or individual chapters and tools can be given to specific staff.

How to use the handbook?

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

Chapter 1: introduces the concept of SIIM and how it fits into the broader security risk management of an organisation.

Chapter 2: presents four key objectives of SIIM, highlighting key steps involved in the effective management of security incident information to achieve each objective.

Chapter 3: is a collection of tools, which are referenced throughout the text and aim to support organisations in the practical application of the guidance shared in the handbook.

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

Specifically, a proper implementation of a security incident information management system will allow the organisation to better:

1. **Inform immediate reaction and response to a security incident (Objective one).** 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.

2. **Implement lessons learned after a security incident for follow-up action and prevention (Objective two).** 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.

3. **Understand the NGO security context (Objective three).** 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.

4. **Inform strategic decision-making in an organisation (Objective four).** 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.
The handbook provides guidance on the key steps under each objective, and shares recommendations on 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.

**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.**

**What are the most useful SIIM handbook sections for you?**

The table in the next pages highlights the sections of the handbook that might be the most relevant to you, based on your position within the organisation and your key responsibilities in relation to SIIM. Click on the position title to go directly to the relevant section of the table.

---

### You are a:

- Security focal point at field or country level
- Security focal point at regional level
- Security manager at HQ level
- Programme manager
- HR specialist
- Finance and funding specialist
- Advocacy and communications specialist
- Strategic decision-maker (directors, board of trustees, etc.)

---

Sections and tools within the *SIIM Handbook*, can be accessed directly from this User Guide. Download the *SIIM Handbook* from the RedR website [here](#) and click on the relevant section or tool in the following pages to reach it directly.
You are a: Security focal point at field or country level.
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</th>
<th>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</th>
</tr>
</thead>
</table>
| **Section:** Key challenges in security incident information management | **Sections:** Guidance on how to report an incident  
Dealing with stress  
Security incident follow-up process  
Dealing with sensitive cases: sexual violence against staff | **Sections:** Post incident analysis  
Implementing lessons learned  
Analysis and follow-up of sensitive cases | **Sections:** External sharing of incident information  
Forums for sharing security incident information |
| **Tool 1:** Self-assessment grid | **Tool 2:** Typology of incidents | **Tool 5:** Incident analysis grids  
**Tool 8:** Action plan for incident follow-up |
| **Tool 4:** Incident reporting template  
**Tool 6:** How to conduct a factual debriefing  
**Tool 10:** Incident storing |

You are a: Security focal point at field or country level.
You are a: Security focal point at regional level.
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</th>
<th>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sections:</strong> Key challenges in security incident information management</td>
<td><strong>Sections:</strong> Guidance on how to report an incident</td>
<td><strong>Sections:</strong> Post incident analysis</td>
<td><strong>Sections:</strong> External sharing of incident information</td>
</tr>
<tr>
<td></td>
<td>Dealing with stress</td>
<td>Implementing lessons learned</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security incident follow-up process</td>
<td>Analysis and follow-up of sensitive cases</td>
<td></td>
</tr>
<tr>
<td><strong>Staff security competencies and SIIM</strong></td>
<td><strong>Dealing with sensitive cases:</strong> sexual violence against staff</td>
<td><strong>Tool 5:</strong> Incident analysis grids</td>
<td></td>
</tr>
<tr>
<td><strong>Information security</strong></td>
<td><strong>Systematic recording of incidents, what system to use?</strong></td>
<td><strong>Tool 8:</strong> Action plan for incident follow-up</td>
<td></td>
</tr>
<tr>
<td><strong>Duty of care</strong></td>
<td><strong>Tool 2:</strong> Typology of incidents</td>
<td><strong>Tool 12:</strong> Analysing and comparing data trends</td>
<td></td>
</tr>
<tr>
<td><strong>Tool 1:</strong> Self-assessment grid</td>
<td><strong>Tool 4:</strong> Incident reporting template</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Sections:
- Key challenges in security incident information management
- Staff security competencies and SIIM
- Incident management and SIIM: the benefits of organisational preparedness
- Duty of care

#### Tool 1:
Self-assessment grid

### Sections:
- Systematic recording of incidents, what system to use?
- Dealing with sensitive cases: sexual violence against staff

#### Tool 2:
Typology of incidents

#### Tool 3:
Organisational or external incident

#### Tool 4:
Incident reporting template

#### Tool 6:
How to conduct a factual debriefing

#### Tool 7:
Good practices in gender-sensitive incident reporting and complaint mechanisms

#### Tool 9:
SIIM systems

### Sections:
- Post incident analysis
- Implementing lessons learned
- Analysis and follow-up of sensitive cases
- Analysis of trends to inform strategic decision making
- How to use incident information on sexual violence at a strategic level
- Using security incident information for strategic advocacy

#### Tool 8:
Action plan for incident follow-up

#### Tool 10:
Incident storing

### Sections:
- External sharing of incident information
- Forums for sharing security incident information
- External contextual trend analysis resources
- Organisational structures to discuss strategic security issues

#### Tool 11:
Technology to report and record incidents

#### Tool 12:
Analysing and comparing data trends

#### Tool 13:
Strategic level questions for incident information management related decisions
### You are a: Programme manager
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th><strong>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</strong></th>
<th><strong>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</strong></th>
<th><strong>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</strong></th>
<th><strong>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</strong></th>
</tr>
</thead>
</table>
| **Sections:** Key challenges in security incident information management | **Sections:** Guidance on how to report an incident  
Dealing with stress  
Security incident follow-up process  
Dealing with sensitive cases: sexual violence against staff  
**Tool 2:** Typology of incidents  
**Tool 3:** Organisational or external incident  
**Tool 4:** Incident reporting template  
**Tool 6:** How to conduct a factual debriefing  
**Tool 7:** Good practices in gender-sensitive incident reporting and complaint mechanisms  
**Tool 9:** SIIM systems  
**Tool 10:** Incident storing  
**Tool 11:** Technology to report and record incidents | **Sections:** Post incident analysis  
Implementing lessons learned  
Analysis and follow-up of sensitive cases  
Analysis of trends to inform strategic decision making  
Using security incident information for strategic advocacy  
**Tool 5:** Incident analysis grids  
**Tool 8:** Action plan for incident follow-up  
**Tool 9:** SIIM systems  
**Tool 12:** Analysing and comparing data trends | **Sections:** External sharing of incident information  
Forums for sharing security incident information  
External contextual trend analysis resources  
Organisational structures to discuss strategic security issues  
**Tool 9:** SIIM systems  
**Tool 12:** Analysing and comparing data trends |

You are a: Programme manager
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th><strong>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</strong></th>
<th><strong>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</strong></th>
<th><strong>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</strong></th>
<th><strong>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</strong></th>
</tr>
</thead>
</table>
| **Sections:** Key challenges in security incident information management | **Sections:** Guidance on how to report an incident  
Dealing with stress  
Security incident follow-up process  
Dealing with sensitive cases: sexual violence against staff  
**Tool 2:** Typology of incidents  
**Tool 3:** Organisational or external incident  
**Tool 4:** Incident reporting template  
**Tool 6:** How to conduct a factual debriefing  
**Tool 7:** Good practices in gender-sensitive incident reporting and complaint mechanisms  
**Tool 9:** SIIM systems  
**Tool 10:** Incident storing  
**Tool 11:** Technology to report and record incidents | **Sections:** Post incident analysis  
Implementing lessons learned  
Analysis and follow-up of sensitive cases  
Analysis of trends to inform strategic decision making  
Using security incident information for strategic advocacy  
**Tool 5:** Incident analysis grids  
**Tool 8:** Action plan for incident follow-up  
**Tool 9:** SIIM systems  
**Tool 12:** Analysing and comparing data trends | **Sections:** External sharing of incident information  
Forums for sharing security incident information  
External contextual trend analysis resources  
Organisational structures to discuss strategic security issues  
**Tool 9:** SIIM systems  
**Tool 12:** Analysing and comparing data trends |
You are a: HR specialist
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</th>
<th>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</th>
</tr>
</thead>
</table>
| **Sections:**  
Key challenges in security incident information management  
Staff security competencies and SIIM  
Duty of care | **Sections:**  
Guidance on how to report an incident  
Dealing with stress  
Dealing with sensitive cases: sexual violence against staff | **Sections:**  
Post incident analysis  
Implementing lessons learned  
Analysis and follow-up of sensitive cases  
Analysis of trends to inform strategic decision making  
How to use incident information on sexual violence at a strategic level | **Sections:**  
External contextual trend analysis resources  
Organisational structures to discuss strategic security issues  
Analysing and comparing data trends |

**Tool 2:** Typology of incidents  
**Tool 6:** How to conduct a factual debriefing  
**Tool 7:** Good practices in gender-sensitive incident reporting and complaint mechanisms  
**Tool 5:** Incident analysis grids  
**Tool 12:** Analysing and comparing data trends  
**Tool 13:** Strategic level questions for incident information management related decisions
You are a: Finance and funding specialist
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</th>
<th>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section:</strong> Key challenges in security incident information management</td>
<td><strong>Tool 2:</strong> Typology of incidents</td>
<td><strong>Sections:</strong> Post incident analysis Implementing lessons learned Analysis and follow-up of sensitive cases Analysis of trends to inform strategic decision making <strong>Tool 5:</strong> Incident analysis grids <strong>Tool 12:</strong> Analysing and comparing data trends</td>
<td><strong>Sections:</strong> External contextual trend analysis resources Organisational structures to discuss strategic security issues <strong>Tool 12:</strong> Analysing and comparing data trends</td>
</tr>
</tbody>
</table>
You are a: Advocacy and communications specialist
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</th>
<th>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section:</strong> Key challenges in security incident information management</td>
<td><strong>Section:</strong> Communication Tool 2: Typology of incidents</td>
<td><strong>Sections:</strong> Post incident analysis Analysis and follow-up of sensitive cases Analysis of trends to inform strategic decision making <strong>Tool 5:</strong> Incident analysis grids <strong>Tool 12:</strong> Analysing and comparing data trends <strong>Tool 13:</strong> Strategic level questions for incident information management related decisions</td>
<td><strong>Sections:</strong> Forums for sharing security incident information External contextual trend analysis resources Organisational structures to discuss strategic security issues <strong>Tool 12:</strong> Analysing and comparing data trends</td>
</tr>
</tbody>
</table>
You are a: Strategic decision-maker (directors, board of trustees, etc.)
The following sections and tools are most relevant to your position:

<table>
<thead>
<tr>
<th>YOU WANT TO ASSESS YOUR ORGANISATION’S PRACTICES IN RELATION TO INCIDENT DATA</th>
<th>YOU WANT TO REINFORCE THE COLLECTION OF INCIDENT DATA IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE THE ANALYSIS OF INCIDENT DATA AND ITS USE IN YOUR ORGANISATION</th>
<th>YOU WANT TO IMPROVE DATA SHARING WITHIN AND OUTSIDE YOUR ORGANISATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sections:</strong></td>
<td><strong>Sections:</strong></td>
<td><strong>Sections:</strong></td>
<td><strong>Sections:</strong></td>
</tr>
<tr>
<td>What is security incident information management</td>
<td>Key challenges in security incident information management</td>
<td>Post incident analysis</td>
<td>Forums for sharing security incident information</td>
</tr>
<tr>
<td>Key challenges in security incident information management</td>
<td>Security risk management and SIIM</td>
<td>Analysis and follow-up of sensitive cases</td>
<td>External contextual trend analysis resources</td>
</tr>
<tr>
<td>Security risk management and SIIM</td>
<td>Staff security competencies and SIIM</td>
<td>Analysis of trends to inform strategic decision making</td>
<td>Organisational structures to discuss strategic security issues</td>
</tr>
<tr>
<td>Information security Incident management and SIIM: the benefits of organisational preparedness</td>
<td>Duty of care</td>
<td>How to use incident information on sexual violence at a strategic level</td>
<td>Tool 12: Analysing and comparing data trends</td>
</tr>
<tr>
<td>Tool 5: Incident analysis grids</td>
<td>Using security incident information for strategic advocacy</td>
<td>Tool 13: Strategic level questions for incident information management related decisions</td>
<td></td>
</tr>
</tbody>
</table>

Tool 12: Analysing and comparing data trends