

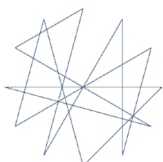
SECURITY INCIDENT INFORMATION MANAGEMENT HANDBOOK

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



Funded by
European Union
Humanitarian Aid

eisf




redruk
people and skills for disaster relief

Aid in Danger



**Insecurity
Insight**

Data on People in Danger



TOOL 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
<p>1. What kind of security incidents did staff and the organisation experience? 2. In which countries did they occur?</p>		
<p>Does our organisation adequately prepare staff for the kind of possible events they may experience?</p>	<p>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.</p>	<p>Suggest the need for specific training or awareness courses for staff working in contexts affected by particular types of incidents.</p>
<p>Does the insurance cover required responses either for staff or to deal with material damage?</p>	<p>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).</p>	<p>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.</p>

<p>QUESTIONS TO THINK ABOUT WHEN LOOKING AT THE ANALYSED SECURITY INCIDENT DATA</p>	<p>POSSIBLE FOLLOW-UP ACTION</p>	<p>POSSIBLE RECOMMENDATION FOR ACTION TO ADD AT THE END OF THE ANALYSIS REPORT</p>
<p>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?</p>		
<p>Are there country offices that may not report systematically to HQ?</p>	<p>Seek a conversation with key personnel to find out why no or only a few incidents were reported.</p>	<p>Recommend the revision of instructions of how and when to report.</p>
<p>Are there country offices that experience particular types of incidents? How do these incidents compare to those experienced by other organisations?</p>	<p>Seek a conversation with key personnel to find out why particular incidents occur frequently or never.</p>	<p>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.</p>
<p>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?</p>		
<p>Have your colleagues reported the extent to which the incidents caused disruption to your work?</p>	<p>Seek conversations with colleagues on how best to describe the impact of security incidents on the delivery of aid.</p>	<p>Add statements on how security incidents affected the delivery of aid.</p>
<p>Have your colleagues costed the loss in staff time and material loss?</p>	<p>Seek conversations with staff of how best to cost the loss of staff time and material goods.</p>	<p>Add statements of the costs of security incidents to operations.</p>
<p>Have your colleagues reported the extent to which the security incident affected access?</p>	<p>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.</p>	<p>Add statements of how security incidents affect access to beneficiary populations.</p>
<p>7. What were the main contexts of security incidents? 8. Can the context of incidents be classified by what response strategy may be needed?</p>		
<p>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?</p>	<p>Seek conversations within the organisation of the best acceptance strategy and how to implement it effectively.</p>	<p>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.</p>

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
<p>7. What were the main contexts of security incidents? 8. Can the context of incidents be classified by what response strategy may be needed?</p>		
<p>How many incidents may have happened because staff disrespected rules or regulations or behaved irresponsibly?</p>	<p>Seek conversations within the organisation of how best to promote ethical code of conducts for staff and ensure adherence to security procedures.</p>	<p>List behaviour aspects that might to be included into a code of conduct staff is required to adhere to.</p> <p>List areas of behaviour where staff disrespected rules and suggest mechanism for better enforcing them.</p>
<p>How many incidents may have happened because of personal factors related to the origin, background or family connections of the staff member?</p>	<p>Seek conversations within the organisation of how to address risk factors related to domestic life, ethnic origin or other private factors.</p>	<p>List contexts and countries where specific policies and procedures may be needed these could include:</p> <ul style="list-style-type: none"> • 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.
<p>How many incidents happened because the staff or the organisation happened to be in the wrong place at the wrong time?</p>	<p>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.</p>	<p>List countries with heightened risk of incidents that are beyond the control of even the best security policies.</p>
<p>How many incidents happened due to action by state actors?</p>	<p>Identify the state actors responsible in internal documents and try to identify avenues to seek a dialogue with these state actors.</p> <p>Talk to advocacy colleagues and consider developing a joined campaign with other NGOs to raise awareness.</p>	<p>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).</p> <p>Identify areas where an organisation could consider an advocacy campaign with others, such as the bombing of infrastructure or impunity from prosecution.</p>

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