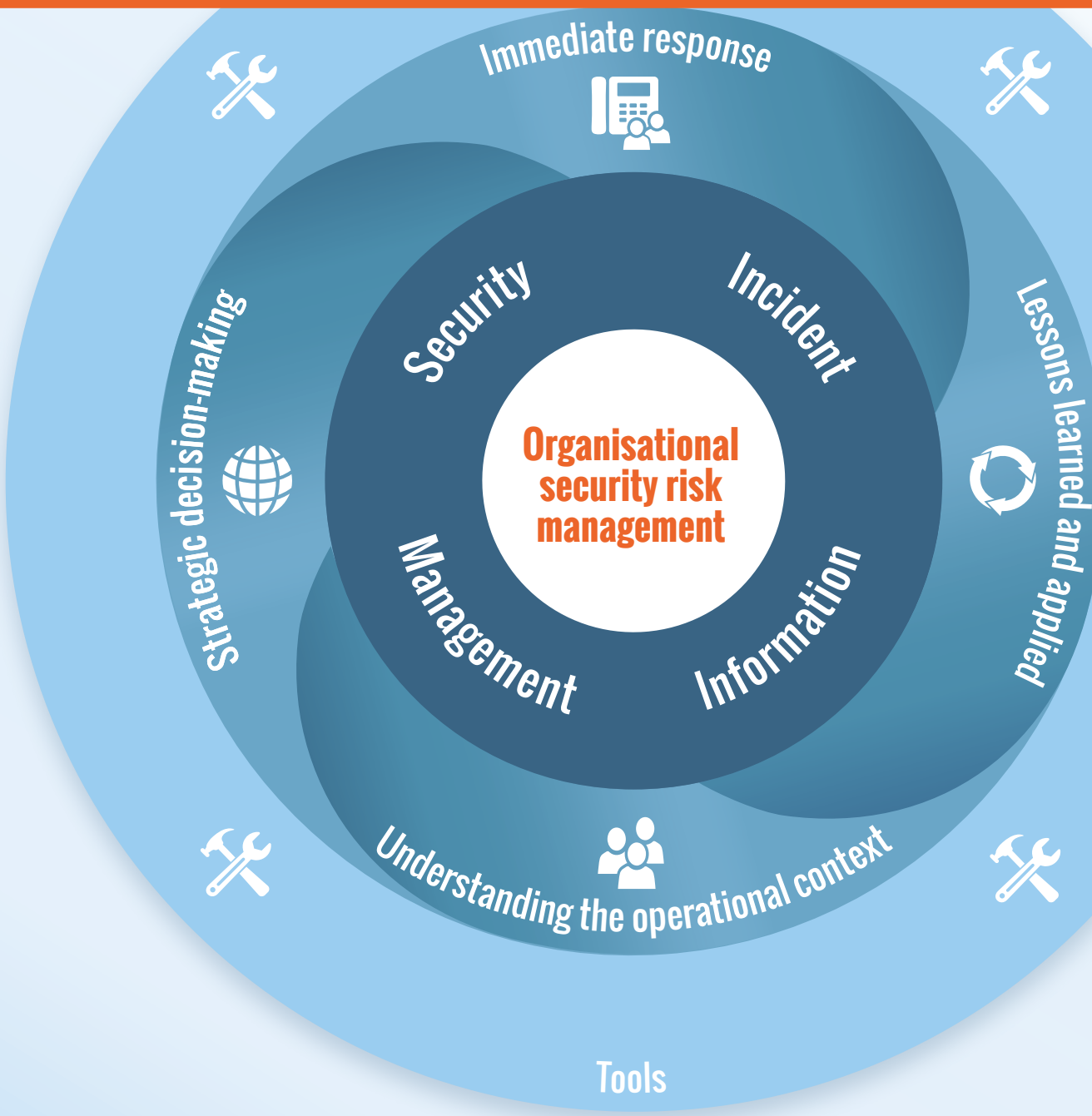
SECURITY INCIDENT INFORMATION MANAGEMENT HANDBOOK

TOOL 12: ANALYSING AND COMPARING DATA TRENDS



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

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.