



## Session

**Basic Security & Safety Awareness**Duration: **3 hours****Session Summary**

This session aims to introduce participants to the approach, behaviours and actions required to minimise security and safety risks in the operating context.

**Session Objectives**

- Highlight key threats in the operating environment and identify the risks to staff and programmes.
- Outline an organisation's approach, procedures, and responsibilities for managing risk.
- Emphasise the importance of developing and maintaining good personal security awareness.
- Describe security and safety measures and procedures at facilities, while travelling and for securing information.
- Discuss basic precautions and immediate response actions for different threat scenarios.
- Explain how to report incidents and an organisation's response to incidents involving staff.

**Learning Outcomes**

By the end of this session, participants should be able to:








- Outline the security and safety threats within the operating context, and list risks to humanitarian aid workers.
- Describe the approach adopted by organisations to manage risk and their duty of care obligations.
- Define the roles and responsibilities of individuals, management and the organisation, with regards to staff security and safety.
- List appropriate actions and behaviours that enhance security and safety within the operating context.
- Identify how to report incidents and describe the support available during an emergency.





**Supporting Material**





- [GISH Security to go: a risk management toolkit for humanitarian aid agencies.](#)
- [GISH Security Risk Management: a basic guide for smaller NGOs.](#)




Time	Suggested Activities	Resources
2 mins	<b>Welcome</b> Welcome participants and introduce the training. Introduce yourself and any other facilitators. If participants are not known to each other, ask participants to introduce themselves. Go round the room with each person saying their name, organisation (if relevant) and job title. Provide details of facilities (toilets, wi-fi, etc.) and explain any important safety measures, including what to do in case of fire alarm or the need to evacuate the building.	<ul style="list-style-type: none"> <li>• Basic Security &amp; Safety Awareness Presentation - Slide 1</li> </ul>
5 mins	<b>Aim, Learning Outcomes &amp; Agenda</b> The aim of the training is to introduce participants to the approach, behaviours and actions required to minimise security and safety risks	<ul style="list-style-type: none"> <li>• Slides 2-3</li> </ul>



	in the operating context. Go through some of the key learning outcomes and deal with any questions or concerns.	
3 mins	<p><b>Security vs Safety</b></p> <p> Ask participants: <i>What is the difference between security and safety?</i></p> <p>Reveal to participants the different definitions for security and safety on the slide and discuss how there is often overlap between the two definitions. If the session is an internal training, discuss how your organisation defines the difference.</p> <p> Security means freedom from harm, or the risk of harm, which results from intentional acts. In humanitarian contexts, these risks might be kidnappings or bombings.</p> <p>Safety means freedom from harm, or the risk of harm, which results from unintentional acts. In humanitarian contexts, these risks might be natural disasters or road traffic incidents.</p> <p>It is also important to note that risks are not only physical but include psychological trauma and mental illnesses.</p> <p>There are many overlaps in the measures required to manage both security and safety risks. Critical safety incidents, such as vehicle accidents, may have additional security implications.</p>	• Slide 4
10 mins	<p><b>Context &amp; Threats</b></p> <p>Use a map of the operational area to highlight factors that shape the current security and safety situation. For example, show key areas or locations affected by violence and insecurity, crime, or the main environmental hazards, any movement restrictions, or obstructions to humanitarian access, and identify the key actors and groups involved.</p> <p>Discuss the different security and safety threats within the operating context. Explain how, when, where, and why some threats might occur, and draw attention to any significant incidents that have occurred.</p>	• Slides 5-6
15 mins	<p><b><i>ACTIVITY: Understanding Risk</i></b></p> <p>Agree with participants ten threats (slide 6) in the operating context to evaluate further. Divide participants into small groups of three or four people. Issue each group a number pyramid (as shown below) on a flip chart sheet and 10 sticky notes.</p> <div data-bbox="526 1610 908 1890" data-label="Diagram"> <pre> graph TD     1[1] --- 2[2]     1 --- 3[3]     2 --- 4[4]     2 --- 5[5]     3 --- 5     3 --- 6[6]     4 --- 7[7]     4 --- 8[8]     5 --- 8     5 --- 9[9]     6 --- 9     6 --- 10[10]     7 --- 10     8 --- 10     9 --- 10     10 --- 10 </pre> </div> <p>Ask each group to write the agreed threats on sticky notes (one per sticky note to create a set of 10 threats). Explain that you want each group to consider the likelihood of each threat occurring to them or their colleagues and its impact if it did. Groups should assess which</p>	Flip chart sheets (one per group) prepared with number pyramids




	<p>threats are most likely to occur, and will cause the greatest harm, to rank risks in their operating context. Groups should then place their sticky notes onto the number pyramid in order of risk - the most serious risk being number 1 and so on). Give the groups 5 minutes to complete this activity.</p> <p>Ask each group to report back on the top three risks they decided on and to explain their reasoning.</p> <p>In plenary, discuss similarities/differences between the different risk pyramids. Provide feedback on key differences and similarities, challenge any misconceptions, and clarify questions raised during the group discussions.</p>	
5 mins	<p><b>Duty of Care</b></p> <p>Briefly explain an organisation's duty of care obligations towards its staff, what this entails, and draw attention to the need to raise awareness and seek informed consent.</p> <p> Duty of care is a moral, ethical, and legal obligation on an organisation to ensure a safe working environment for its staff, or those working on its behalf, including volunteers, interns, contractors (such as guards or drivers), and also implementing partner organisations - although the level of duty of care required may be different.</p>	• Slide 7
5 mins	<p><b>Management of Risk</b></p> <p>Explain the factors that shape an organisation's attitude to risk and its overall approach to managing risk. If an internal training, include references to your organisation's specific approach to managing risk.</p> <p> The approach is not simply to avoid risk, but to manage risk in a way that allows staff, and the organisation, to remain present and effective in those locations.</p> <p>To ensure secure access to affected populations, the organisation adopts a range of safety and security approaches depending on the specific risk in a country or particular location.</p>	• Slide 8
20 mins	<p><b>ACTIVITY: Who's Responsible?</b></p> <p> Ask participants: <i>Who is responsible for the security and safety of staff?</i></p> <p>After a few initial suggestions, move on to the exercise. Split participants into three groups. Explain that you want participants to consider the key security and safety responsibilities associated with different levels within an organisation:</p> <ul style="list-style-type: none"> <li>• Organisational (HQ)</li> <li>• Management (Country Office)</li> <li>• Individual (Staff)</li> </ul> <p>Allocate one level to each group. Ask participants to represent different security and safety responsibilities for their level in the form of pictures</p>	• Slide 9

	<p>only – no words – on a flip chart sheet. Give them a maximum of 10 mins to quickly identify and draw some responsibilities for their level.</p> <p>Once completed, each group should present and explain their pictures to other groups. Ask others if there are any key responsibilities missing for that level.</p> <p>To conclude the exercise, emphasise the shared responsibility individual staff have to manage and reduce risks to all staff.</p> <p> Managing risk to staff is a shared responsibility. Every staff member has a responsibility for their own safety and security, and for their colleagues.</p>	
5 mins	<p><b>Acceptance-based Approach</b></p> <p>Explain how building acceptance and maintaining consent for an organisation's presence and activities is one of the main risk-reducing strategies adopted by humanitarian agencies. If an internal training, explain how an acceptance-based approach shapes your organisation's security strategy.</p> <p> An acceptance-based approach involves building positive relationships and creating awareness and support for the organisation's work amongst beneficiaries, community leaders, local authorities, security forces and, in some cases, armed groups or others who may wish to obstruct programme implementation or harm staff. Such an approach can help gain and maintain acceptance and support for the organisation's presence and its activities, which will ultimately improve security and access for staff.</p> <p>Emphasise the vital role individual staff have in gaining and maintaining levels of acceptance through their personal behaviour and conduct.</p> <p> Ask participants: <i>What are some of the challenges to gaining and maintaining acceptance within the operating context?</i></p> <p>Draw attention to the difficulties in gaining acceptance from certain groups in the operating context, and the need to use other strategies (protection and deterrence) and implement procedures and measures that reduce staff vulnerability to risks.</p>	<ul style="list-style-type: none"> <li>• Slide 10</li> </ul>
10 mins	<p><b>Inclusive Security</b></p> <p>Write the following statement on a flip chart – “All staff face risks but not all staff face the same risks”. Present the statement to participants and ask them to explain the statement. Explain that individuals may face different risks or be more vulnerable to certain threats because of their profile or identity.</p> <p> Ask participants: <i>What aspects of an individual's profile or identity may make them more vulnerable to specific threats?</i></p> <p>Highlight key elements from their contributions on the flip chart. For example, the importance of the profile of the staff member, their nationality, ethnicity, gender, sexual orientation, ability, etc.</p> <p>Describe the diversity of people who work within aid organisations in general, or your organisation, and highlight some of the risks they face.</p>	<ul style="list-style-type: none"> <li>• Slide 11</li> </ul>

	<p>Describe an inclusive approach to security.</p> <p>An inclusive approach to security acknowledges the risks that individuals with diverse profiles may face, and actively provides them with the guidance and support they need to enable them to fully participate and feel protected.</p>	
5 mins	<p><b>Security Plans &amp; Procedures</b></p> <p>Explain the purpose of security plans, their key contents, and how they support security management within different locations. Highlight that these documents may have different titles, depending on the organisation. If internal training, adapt the slides to reflect the title of the documents used in your organisation.</p> <p> Security plans are key country-level documents that outline the security and safety measures and procedures in place, and the responsibilities and resources required to implement them.</p> <p>Refer participants to examples of country/area security plans, or if an internal training, your organisation's current security plan for their location.</p>	• Slide 12
5 mins	<p><b>Basic Security Principles</b></p> <p>Outline the basic principles that all staff should routinely adhere to, in order to minimise risks to themselves and their colleagues.</p> <p>Emphasise the importance of “Aware – Prepare – React!”</p> <p></p> <ul style="list-style-type: none"> <li>• Aware – monitor your surroundings and be alert to any changes occurring that affect your security or safety.</li> <li>• Prepare – anticipate things that could occur and be prepared should they happen.</li> <li>• React – know how to react and what immediate actions to take should anything happen.</li> </ul>	• Slide 13
10 mins	<p><b>Site Security &amp; Safety</b></p> <p> Ask participants: <i>What threats do you face while in the office, other workplace, or your residence?</i></p> <p>Capture suggestions on a flip chart, and add threats not raised by participants. Draw attention to any specific incidents that have affected your organisation, or others in the same location.</p> <p>Emphasise why it is important to establish a safe and secure workplace for staff.</p> <p> It is vital that staff feel safe and secure in their workplace, and in their residence or guesthouse. Effective controls and procedures must be in place, and adhered to, for security and safety risks to be minimised.</p> <p>Explain that security and safety at various facilities and workplaces is managed through a mixture of physical measures and procedures.</p>	• Slide 14

	<p>Briefly explain the guarding arrangements and access controls used at facilities in that location. Emphasise the role of guards, and the responsibilities of individual staff.</p> <p>Explain the risk posed by fires and draw attention to specific factors in that location that may increase the risks to staff and property. Outline the essential measures staff should take to prevent fires and how to safely respond if one occurs.</p> <p>Briefly explain the key emergency procedures that apply to NGO offices in general, or your organisation's office if an internal training. Draw attention to the alarms and alerts in place, where and how staff should evacuate the building, including muster points and the warden system in place.</p>	
10 mins	<p><b>Staff Travel &amp; Movements</b></p> <p> Ask participants: <i>What threats do you face while travelling in the areas you work?</i></p> <p>Capture suggestions on a flip chart, and add threats not raised by participants. Draw attention to any specific incidents that have affected your organisation, or others in the same location.</p> <p>Explain why preparation and planning is key to safe and secure staff movements.</p> <p> Be prepared! Know the risks, and plan accordingly.</p> <p>Highlight the essential measures and behaviours that staff should undertake prior to travelling, and during trips to other offices or project areas. Explain the communication systems used, and how and when to maintain contact while travelling. Adapt the list on the slide to reflect the operating environment and include any specific requirements within that location. If an internal training, draw attention to your organisation's requirements.</p>	<p>• Slide 15</p>
5 mins	<p><b>Information Security</b></p> <p>Stress the need to be security-conscious when collating, storing, communicating, and disposing of sensitive information. Provide examples of sensitive information in that location.</p> <p>Explain that securing information requires a combination of three key elements - Physical Security, Digital Security and Communications Security. Provide examples of the different elements that are relevant for the local context, or your organisation.</p> <p> Information security is comprised of a layered approach, with several barriers to protect information from loss, theft and unauthorised access or disclosure:</p> <ul style="list-style-type: none"> <li>• Physical Security - locked filing cabinets, 'clear desk' policies, visitor procedures, secure disposal of documents.</li> <li>• Digital Security - password protection and encryption, restricted access to folders/files, backing-up systems, secure disposal of computers and data storage devices.</li> </ul>	<p>• Slide 16</p>

	<ul style="list-style-type: none"> <li>• Communications Security - secure communication practices, splitting information, using secure email and file-transfer systems.</li> </ul> <p>Highlight the risks associated with using social media. Provide basic guidance staff should follow when interacting and posting online to prevent additional security risks for themselves or their colleagues.</p>	
30 mins	<p><b>Dealing with Incidents</b></p> <p>Identify two or three key threat topics to focus on. Choices will be influenced by the threats in the operating environment. A choice of different threat slides can be found in the Personal Security &amp; Safety Training PowerPoint presentation (S.10 Dealing with Incidents), and the relevant slides can be pasted into this presentation.</p> <p>For each threat discussed, provide an overview of that threat and its potential impact. Where possible, draw attention to any incidents within the operating context to emphasise how and when they are likely to occur, and who is most likely to be affected.</p> <p>Highlight some of the measures and actions staff can take to prevent such incidents or, should they occur, how to respond to minimise their impact.</p> <p> When faced with threatening situations, how effectively you respond and deal with the situation is influenced by how alert and prepared you are. Individuals respond much better if they have thought about a threat beforehand and considered how best to respond. Similarly, if teams discuss likely scenarios and agree in advance how best to respond if they occur, it is more likely that individuals in a team will react in a similar way.</p>	<ul style="list-style-type: none"> <li>• Slide 17</li> <li>• PSS S.10 Dealing with Incidents Presentation (only use slides that relate to threats chosen).</li> </ul>
5 mins	<p><b><i>ACTIVITY:</i> Incident or Not?</b></p> <p>Divide the participants into pairs, ask them to review the different scenarios and consider:</p> <ul style="list-style-type: none"> <li>• <i>Would they report it?</i></li> <li>• <i>If yes, when would you report it, how and to whom?</i></li> </ul> <p>After a few minutes, ask participants for their answers to the different scenarios. Ask each pair to provide their response to one scenario, moving around the group until all scenarios are answered.</p> <p>All are reportable incidents - the only difference is when they would be reported, how they are reported, and to whom.</p> <p> If you are in any doubt whether something it is a security or safety incident, report it anyway and let others decide. What may seem an isolated and insignificant incident may in fact signify a significant threat to staff when viewed in the context of other incidents or events.</p>	<ul style="list-style-type: none"> <li>• Slide 18</li> </ul>
5 mins	<p><b>Reporting Incidents</b></p> <p>Explain the importance of reporting incidents and how this helps to protect staff, improves understanding and decision-making, and ultimately improve programmes. Provide some examples of what</p>	<ul style="list-style-type: none"> <li>• Slide 19</li> </ul>

	<p>reportable incidents are in that location and emphasise the need to also report 'near misses'.</p> <p> Perceptions of what represents 'an incident' will vary greatly between staff members and locations, depending on what is considered the norm in that context. 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.</p> <p>'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.</p> <p>If an internal training, explain the organisation's incident reporting procedures in that location, who incidents must be reported to, when and in what format.</p>	
10 mins	<p><b>Critical Incident Support</b></p> <p>Draw attention to an organisation's incident management structures (titles will vary, so if an internal training remember to adjust slides to reflect your organisation's own structure) and briefly explain how these structures respond to critical incidents involving staff.</p> <p> Most incidents will be handled through regular line management. However, critical incidents require a dedicated structure to respond, due to their nature and severity, or wider implications for the organisation. The country-level Incident Management Team (IMT) and HQ Crisis Management Team (CMT) would manage all aspects of a critical incident, liaising with different stakeholders and providing support to the victims and their family members.</p>	<ul style="list-style-type: none"> <li>• Slide 20</li> </ul>
15 mins	<p><b>Wrap-up &amp; Review</b></p> <p>Explain that in such a short security training there are many topics that could not be included or discussed.</p> <p> Ask participants: <i>Are there any security or safety issues you would like further information or clarity on?</i></p> <p>Provide further information or advice in response to questions raised. Refer to the slide showing the Learning Outcomes to quickly review what participants should be taking away with them.</p> <p>Issue each participant with three sticky notes in different colours. Explain that you would like them to provide some feedback on the training. Ask them to write on each sticky note something they <b>Learned</b> during the training, something they <b>Liked</b> about the training, and finally something they would <b>Suggest</b> to improve the training. Explain which colour of sticky note applies to which feedback.</p> <p>Let participants know that you welcome further feedback by email or informally as people depart.</p> <p>Conclude the training by thanking participants for their participation.</p>	<ul style="list-style-type: none"> <li>• Slide 3</li> </ul>