

Security & Safety Training Pack

Published on 10 March 2022



The GISF Security & Safety Training Pack provides ready-made resources and comprehensive guidance to support security staff in delivery of security training.

The training pack's modular format enables security and safety training to be adapted to the local operating environment, the threats that exist, and the needs of different staff.



Download a PDF version of the GISF Security & Safety Training Pack (807KB)

Disclaimer

GISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'GISF' in this disclaimer shall mean the member agencies, observers and secretariat of GISF.

The content of this document is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this document.

While GISF endeavours to ensure that the information in this document is correct, GISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk.

Accordingly, to the maximum extent permitted by applicable law, GISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. GISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

Introduction

Training is a vital part of improving the security awareness and management capacity of staff. Many NGOs understand the importance of security training; in practice, however, the cost, time and capacity of security staff to deliver training remain significant barriers to organisations implementing and sustaining security training for staff at the local and national levels. Smaller NGOs, in particular, with limited resources and security capacity, can struggle to provide much needed security training to staff.

While security staff are keen to establish and provide security training to staff, they are often time-constrained or have limited training experience. Therefore, developing training materials, and considering which topics to cover and how, can be an additional barrier, especially in an emergency setting when there is a need to quickly provide training to large groups of staff across many different locations.

Although some larger organisations already have well established security training programmes and provide security training resources for staff to deliver in their different offices, many do not.

The GISF Security & Safety Training Pack provides ready-made resources and comprehensive guidance to support security staff in the delivery of security training. The training pack is designed in a modular format so that the resources can be adapted to the training needs in different locations.

Who is this resource for?

The training pack is aimed principally at country-level security staff who are looking to facilitate security and safety training for their staff, or for staff from other organisations and local partners as part of a wider security collaboration initiative.

Although the resources were developed for country level training, the pack can also be used to support organisations in establishing security training at HQ or for international travelling staff, as much of the content is easily adaptable for different audiences.

How to use the materials

This pack provides flexible resources that can be contextualised to the local operating environment, the threats that exist, and the training needs of different staff. The programmes include three distinct levels of training: a short basic security and safety awareness training, a personal security and safety training, and a security management training.

Each training programme includes detailed session plans with learning outcomes and suggested activities and delivery times, PowerPoint presentations, handouts, and links to supporting material. The packages also provide practical guidance on delivering security and safety training in different locations, and will help security staff plan, deliver and evaluate their own training programmes.

Sections of the pack can also be used to support existing training programmes or activities, or to deliver standalone security and safety training. In situations where face to face training is not possible or feasible, the training materials and exercises can easily be adapted for delivery remotely, using video conferencing platforms.

Acknowledgements

The training pack was developed by Shaun Bickley ([Tricky Locations](#)) with input from Lisa Reilly, GISF Executive Director.

GISF would like to thank the following people who contributed their time and expertise to the development of these materials: Anne-Céline Okonta (Action contre la Faim), Gonzalo de Palacios (Oxfam International), Martin Hartney (Catholic Relief Services), Mike Croll (Tearfund), Peter Sjøstedt (Danish Refugee Council) and Philipp Burtzlaff (CBM).

1. Facilitator guide

This guide supports facilitators as they prepare to deliver security training programmes. It provides advice and information on how to plan, organise and conduct the training and how to adapt the material.

Assessing need

Before undertaking any type of learning event, you should conduct a Learning Needs Assessment (LNA) to better understand the security training requirements of different groups of staff or organisations within the planned location. The LNA also helps you to define the content and structure of the training.

It is also crucial to identify the specific security and safety challenges faced by aid organisations and staff in that location, so the sessions can be adjusted to ensure that these issues are addressed appropriately.

Planning training

How you plan and deliver the training programmes will depend on the context, the participants, and the time available. The time suggested for each programme reflects the minimum hours required to deliver the content. However, it is intended to be flexible, and the training could be spread out over a longer period, for example the Personal Security & Safety Course could be run as a two-day course. Indeed, this is actively encouraged, as it would provide more time for discussion, exercises, and additional content.

Training methodology

All security programmes within the training pack use participatory methods including group work, small group discussion, case studies, videos clips and presentations. The session plans also provide links to additional resources that can be used to reinforce the learning.

Agenda

The training pack provides sample agendas for each of the different training programmes. You should adapt the agendas and the timings of the different sessions to suit the working day, and timings of breaks and lunches, within the planned location.

Group size

Each programme is designed to maximise participation through group work and small group discussion, so it is important to keep the number attending relatively small, ideally no more than 20 participants. A smaller group enables you to ensure all participants are engaged during discussions, and that feedback time from the exercises does not overrun into other sessions. Should the training audience need to be much larger, you will need to make adjustment to the session timings and size of working groups.

Training venue and room layout

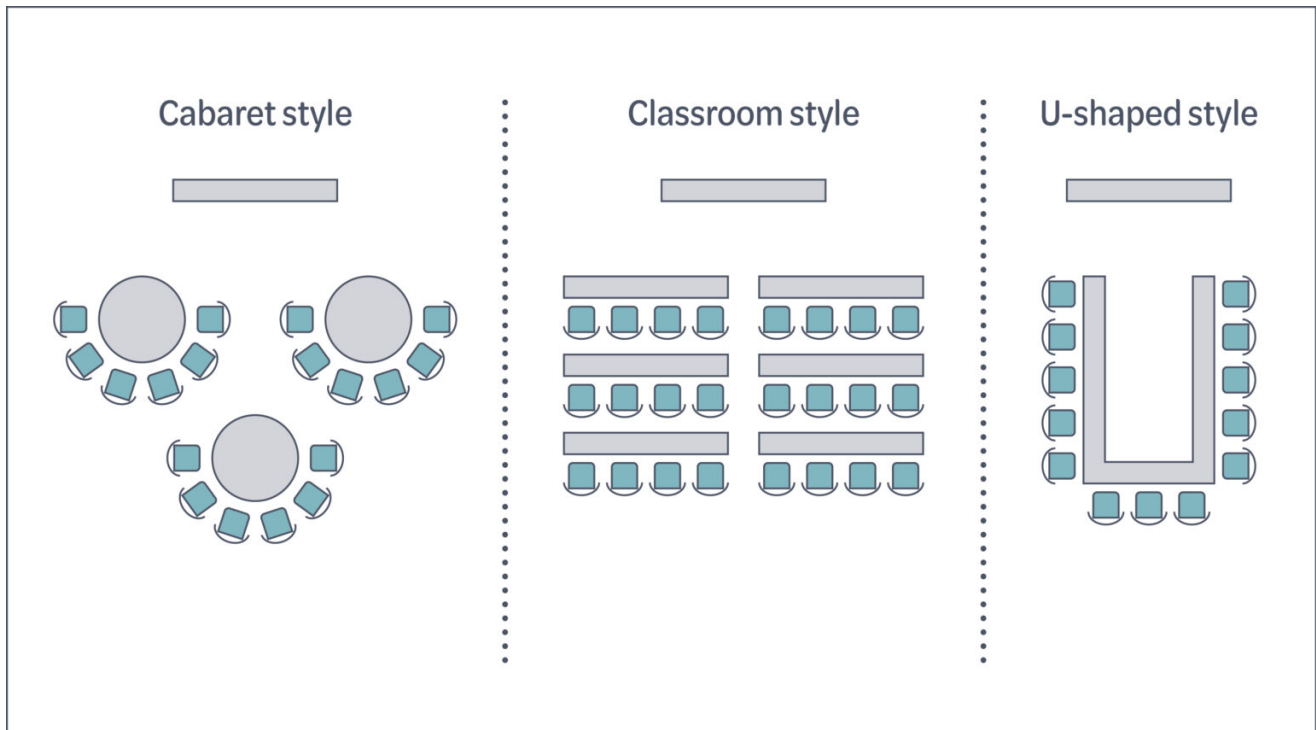
Selecting a suitable venue for training is important. If there is sufficient space within your office, you can use this space. While this helps to minimise the costs, it does have some drawbacks, allowing participants to be distracted by their daily duties.

If you plan to use an external venue, there are a few things to consider:

- **Ensure the venue is in a secure area** – make sure that the location is easily and safely reached by all participants.
- **Plan for adequate space** – there should be space for general sessions and breakout areas for group work.
- **Ensure the space is accessible** – the building and its accessibility should suit the diversity of prospective participants, including wheelchair users.
- **Confirm that the space is suitable for productive learning** – the rooms should be large enough for the number of participants, be away from other events and distracting noise, with natural light so people remain engaged, and with refreshments and toilets located nearby.
- **Check the audio-visual and technology available** – check the venue has audio-visual equipment, internet/wireless access (with sufficient bandwidth), consistent power supply, and that the rooms are air conditioned or heated.
- **Conduct a site visit** – if possible, visit the venue beforehand to confirm that it meets your needs and to familiarise yourself with the emergency escape plans and routes.

There are various possible configurations for the room. You need to decide the layout that is appropriate for your style, the size and configuration of the room, and the number of participants.

Possible layouts include: 'cabaret or café style', 'classroom style' and 'U-shaped style'.



If the room is not large enough for participants to work in groups, you will need to have additional breakout space for group work. Make sure it is as near to the training room as possible.

Training materials and delivery

The training pack provides all the materials required to deliver different security training programmes. Each programme includes detailed session plans with learning outcomes, suggested activities and timings, exercise handouts, additional information for facilitators, and PowerPoint presentations.

Planning and conducting training requires a significant amount of preparation. It is crucial that you are familiar with the training materials and allocate sufficient time to understand how the sessions flow into each other.

You will also need to spend time ahead of the training adapting the materials to ensure the content is specific to your audience and location. The session plans provide advice on how best to contextualise the material. Use these guides to adapt the slides and exercises to suit the local context and ensure the most relevant information is used.

The time required to facilitate each session depends on the size of the group, the level of experience of the participants, and the topics discussed. To cover the material in the time available, you may need to make adjustments to the specific issues covered in each session. You will need to use your judgment and assess the group to prioritise what to leave out or cover more quickly. Although it is possible to adjust the timing of the breaks (longer/shorter, earlier/later), it is advisable to make sure

you start and end as communicated on the agenda. Try to maintain the right balance of presentations and the discussion exercises.

Adapting materials

While the training materials are designed to be adjusted to suit the local context, and may be tweaked to suit your preferred training style, it is important to make sure that the main learning objectives are covered.

Although session plans contain an overview of the issues and topics to discuss, you are encouraged to add your own anecdotes and experiences to provide contextual learning for the participants. Several exercises make use of generic context examples and can be run as they are, although it is highly recommended to adapt the materials to make them more relevant and realistic to participants' operating context.

Training evaluation

End of training evaluations or reviews are useful to understand how well the training was received and to strengthen future trainings. Verify if participants have understood the materials and topics covered, what they found useful, and what they would recommend for improving the training. It is important to take the evaluations seriously, but at the same time do not take any individual comments personally.

A [sample evaluation form](#) is provided. If you are running internal trainings then use the evaluation forms adopted by your organisation, if available.

Facilitator checklist

- **Read all the materials** – make sure you read all the session plans. Note areas that require additional preparation – handouts, flipcharts, adapting slides and other training materials.
- **Check technology, logistics and access** – ensure you have all the required equipment (visuals and sound), and that they are working. Make sure the room is big enough, with breakout areas, and that refreshments and meals are available. Ensure the space is accessible for all participants and familiarise yourself with the emergency exits.
- **Know the audience** – assess the experience level of the audience and adjust the materials and your approach to suit. Be aware of any existing dynamics among participants or potential challenges, and try to address these before the training starts.
- **Understand cultural norms and learning approaches** – identify the training style that is most appropriate for this group. Ensure a safe learning environment so participants feel respected, and able to share their experiences and raise questions.
- **Be aware of gender dynamics** – where possible, try to ensure a balance of genders in the group to aid discussion and understanding of all.

- **Be mindful of participants' needs** – identify participants with additional needs to ensure there are no barriers to their participation. Confidentially discuss these with the individuals themselves before the training to enable any adaptations required.
- **Be sensitive to participants who may have experienced traumatic incidents** – security training covers topics that can be traumatic, and the subjects discussed may cause a participant to feel uncomfortable. Before and during the training, alert participants to the material to be covered and provide a safe opportunity, in private, for individuals to voice any concerns.
- **Be familiar with adult learning approaches** – remember that participants are experienced adults. Sitting still listening to one person talking can easily drain energy. Participants learn more and enjoy the training more if they can engage and discuss issues with others.
- **Keep the goals in mind** – always keep in mind the overall aim of the training and the learning outcomes. Continue to reference these throughout the training.

2. Training programmes

GISF's Safety & Security Training Pack includes three off-the-shelf training programmes, adjustable to different audiences and timeframes. The training programmes include:



[Basic Security & Safety Awareness](#) – a basic 3 hours security induction/orientation



[Personal Security & Safety](#) – a one day (7 hours) course for staff working in moderate-risk environments



[Security Risk Management](#) – a two-day (14 hours) course aimed at staff with security management responsibilities

Each training programme can be edited and adapted according to need and the local context, and includes detailed session plans, PowerPoint presentations and handouts.

2.1 Basic Security & Safety Awareness



Duration

3 hours



Target audience

All staff and local partners.

Aim

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

Key learning outcomes

By the end of the training, 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; and
- Identify how to report incidents and describe the support available during an emergency.

No.	Title	Time	Topics	Suggested Activities	Resources
1	Introduction	10 mins	<ul style="list-style-type: none"> • Welcome and introductions • Aims, objectives and learning outcomes 	PRESENTATION: Introduction	<ul style="list-style-type: none"> • Basic Security & Safety Awareness – Session Plan (pdf) • Basic Security & Safety Awareness presentation (pptx)
2	Context & Threats	25 mins	<ul style="list-style-type: none"> • Context overview • Threats in the operating environment • Risks to staff and programmes 	PRESENTATION: Context & Threats (10 mins) ACTIVITY: Understanding Risk (15 mins) – simple risk-prioritising exercise.	
3	Managing Risk	50 mins	<ul style="list-style-type: none"> • Duty of care obligations • Management of risk • Shared responsibilities • Acceptance-based approach • Inclusive security • Security plans and procedures 	PRESENTATION: Managing Risk ACTIVITY: Who's Responsible? -drawing exercise and discussion.	

No.	Title	Time	Topics	Suggested Activities	Resources
4	Basic Security & Safety Measures	60 mins	<ul style="list-style-type: none"> • Basic security principles • Site security and safety • Staff travel and movements • Information security • Dealing with incidents 	PRESENTATION: Basic Security & Safety Measures	
5	Incident Reporting & Support	20 mins	<ul style="list-style-type: none"> • Reporting incidents • Critical incident support 	ACTIVITY: Incident or Not? (10 mins) – incident reporting quiz. PRESENTATION: Incident Reporting & Support (10 mins)	
6	Wrap-up & Review	15 mins	<ul style="list-style-type: none"> • Participant Q&A • Participant reflection and feedback 	Plenary Discussion	

2.2 Personal Security & Safety



Duration

1 day (7 hours)



Target audience

Staff and local partners working in insecure environments.

Aim

To develop the personal security and safety awareness of participants to enable them to operate safely within insecure environments.

Key learning outcomes

By the end of the training participants should be able to:

- Outline security and safety threats within the operating environment, and identify the contextual factors that affect risks for humanitarian aid workers;
- Describe the culture and approach adopted by organisations to manage security and safety risks to staff;
- Define the roles and responsibilities of individuals, management, and the organisation with regards to staff security and safety;
- Explain how a person's identity affects their vulnerability to internal and external threats, and describe an inclusive approach to security;
- Describe situational awareness and list appropriate actions and behaviours that enhance security and safety within the operating context;
- Describe the measures and procedures in place to minimise security and safety risks within workplaces and accommodation;
- Recall basic precautions, and security and safety procedures for staff travel and movements within the operating context;
- Recognise the risks associated with managing information and using social media, and list measures to protect sensitive information;

- Outline preventative measures to minimise specific security and safety threats, and describe how to respond to incidents or situations; and
- Recall how to report incidents and explain an organisation's structure and approach to managing incidents.

- [Personal Security & Safety Course – Sample Agenda](#)

No.	Session	Time	Topics	Suggested Activities	Resources
1	Introduction	20 mins	<ul style="list-style-type: none"> • Welcome and introductions • Aims, objectives and learning outcomes • Agreement of ground rules 	<p>PRESENTATION: Introduction (10 mins)</p> <p>ACTIVITY: One Word! (10 mins) – icebreaker.</p>	<ul style="list-style-type: none"> • S.1 Introduction Session Plan • S.1 Introduction Presentation
2	Threats & Risks	40 mins	<ul style="list-style-type: none"> • Context overview • Key threats in the operating environment • Risks to staff and programmes 	<p>PRESENTATION: Threats & Risks (20 mins)</p> <p>ACTIVITY: Understanding Risk (15 mins) – simple risk-prioritising exercise.</p>	<ul style="list-style-type: none"> • S.2 Threats & Risks Session Plan • S.2 Threats & Risks Presentation
3	Security Culture & Approach	30 mins	<ul style="list-style-type: none"> • Duty of care obligations • Management of risk • Acceptance-based approach • Framework, policy and requirements • Security plans and procedures 	<p>PRESENTATION: Security Culture & Approach (15 mins)</p> <p>ACTIVITY: Policy – Fact or Fiction? (15 mins) – mixed statement exercise on common NGO security principles and requirements.</p>	<ul style="list-style-type: none"> • S.3 Security Culture & Approach Session Plan • S.3 Security Culture & Approach Presentation • S.3 Policy – Fact or Fiction? Statement Sheet
4	Shared Responsibilities	30 mins	<ul style="list-style-type: none"> • Individual, management, and organisational responsibilities 	<p>ACTIVITY: Who's Responsible? – drawing exercise and discussion.</p>	<ul style="list-style-type: none"> • S.4 Shared Responsibilities Session Plan

No.	Session	Time	Topics	Suggested Activities	Resources
5	Inclusive Security	30 mins	<ul style="list-style-type: none"> • Diversity in risk • Inclusive security • Measures and support for staff with diverse profiles 	<p>ACTIVITY:Diversity Iceberg (10 mins) – visible vs invisible personal characteristics exercise.</p> <p>ACTIVITY: In Someone Else’s Shoes (5 mins) – simple risk exposure exercise.</p> <p>PRESENTATION: Inclusive Security (15 mins)</p>	<ul style="list-style-type: none"> • S.5 Inclusive Security Session Plan • S.5 Diversity Iceberg Sheet • S.5 In Someone Else’s Shoes – Character Profiles • S.5 Inclusive Security Presentation
6	Personal Awareness & Behaviour	30 mins	<ul style="list-style-type: none"> • Basic security principles • Developing awareness • Essential dos and don’ts • Active bystander 	<p>PRESENTATION: Personal Awareness & Behaviour</p>	<ul style="list-style-type: none"> • S.6 Personal Awareness & Behaviour Session Plan • S.6 Personal Awareness & Behaviour Presentation
7	Site Security & Safety	45 mins	<ul style="list-style-type: none"> • Site-specific threats • Site protection measures • Guards and access controls • Emergency procedures • Fire safety 	<p>ACTIVITY: Game of Threats (15 mins) – site protection exercise.</p> <p>PRESENTATION: Site Security & Safety (30 mins)</p>	<ul style="list-style-type: none"> • S.7 Site Security & Safety Session Plan • S.7 Site Security & Safety Presentation
8	Field Travel & Movements	45 mins	<ul style="list-style-type: none"> • Travel-specific threats • Field movements – basic preparations, on the road, communications • Checkpoints 	<p>PRESENTATION: Field Travel & Movements (30 mins)</p> <p>ACTIVITY: Negotiating Checkpoints (15 mins) – video exercise.</p>	<ul style="list-style-type: none"> • S.8 Staff Travel & Movements Session Plan • S.8 Staff Travel & Movements Presentation
9	Information Security & Privacy	30 mins	<ul style="list-style-type: none"> • Securing information • Digital footprint • Using social media 	<p>PRESENTATION: Information Security & Privacy (20 mins)</p> <p>ACTIVITY: Data Mining (10 mins) – online footprint exercise.</p>	<ul style="list-style-type: none"> • S.9 Information Security Session Plan • S.9 Information Security Presentation

No.	Session	Time	Topics	Suggested Activities	Resources
10	Dealing with Incidents	75 mins	Threat-based modules include: <ul style="list-style-type: none"> • Shooting and crossfire • Blast threats (bombs and IEDs) • Mines and UXO • Violent protests and civil unrest • Intimidation and threats • Sexual violence • Armed robbery • Carjacking • Detention and arrest • Abduction and kidnapping • Road traffic accidents (RTAs) • Environmental hazards 	<p>ACTIVITY: Prevent & Respond (35 mins) – group exercise to identify basic precautions and immediate response actions for different threat scenarios. The threats selected depend on the key risks within the operating context.</p> <p>PRESENTATION: Dealing with Incidents (40 mins) – the threat-based slides used will depend on the threats selected for the Prevent & Respond activity.</p>	<ul style="list-style-type: none"> • S.10 Dealing with Incidents Session Plan • S.10 Dealing with Incidents Presentation
11	Incident Reporting & Support	30 mins	<ul style="list-style-type: none"> • Reporting incidents • What to report • How to report • Critical incident support 	<p>ACTIVITY: Incident or Not? (10 mins) – incident reporting quiz.</p> <p>PRESENTATION: Incident Reporting & Support (20 mins)</p>	<ul style="list-style-type: none"> • S.11 Incident Reporting & Support Session Plan • S.11 Incident Reporting & Support Presentation
12	Wrap-up & Review	15 mins	<ul style="list-style-type: none"> • Participant Q&A • Parked topics/issues • Participant reflection and feedback 	Plenary Discussion	<ul style="list-style-type: none"> • S.12 Wrap-up & Review Session Plan

2.3 Security Risk Management



Duration

2 days (14 hours)



Target audience

Staff with security and safety management responsibilities (Security Focal Points, Field/Project Managers, etc).

Aim

To equip participants with the awareness, skills and tools to manage security and safety risks to staff and programmes, within their specific operating context.

Key learning outcomes

By the end of the training, participants should be able to:

- Discuss the security challenges facing humanitarian aid workers globally and describe an organisational approach to managing its duty of care;

- Recall the key responsibilities, processes and tools involved in a systematic approach to managing security in the operating context;
- Identify the different contextual factors that should be assessed and monitored to understand the overall security situation;
- Use a risk analysis matrix to prioritise threats in the operating environment according to their likelihood and impact;
- Discuss pros and cons of different security strategies and identify an appropriate approach for the operating context and the organisation;
- Explain how diversity considerations affect risks for individual members of staff, and highlight specific measures required to support staff with diverse profiles;
- Recall the contents of a security plan and contribute to the development of effective SOPs and contingency plans;
- List effective security and safety measures for an organisation's facilities;
- Identify essential security and safety procedures for managing vehicle travel, staff movements and communications;
- Describe the essential elements involved in providing effective security orientations and briefings for staff and visitors;
- Identify security and safety costs and explain how security funding should be addressed in proposals and annual budget plans;
- Recall contingency planning requirements for relocating or evacuating staff, and responding to medical emergencies;
- Outline incident reporting requirements and the mechanisms used to manage security incident information; and
- State the structures and stakeholders involved in managing critical incidents and identify various immediate actions and support needs.

- [Security Risk Management Course – Sample Agenda](#)

No.	Session	Time	Topics	Suggested Activities	Resources
1	Introduction	30 mins	<ul style="list-style-type: none"> • Welcome and introductions • Aims, objectives and learning outcomes • Participant expectations • Agreement of ground rules 	<p>PRESENTATION: Introduction (20 mins)</p> <p>ACTIVITY: Expectations (10 mins) – participant expectations exercise.</p>	<ul style="list-style-type: none"> • S.1 Introduction Session Plan • S.1 Introduction Presentation
2	Security & Programmes	45 mins	<ul style="list-style-type: none"> • Operating environment • Aid worker security • Duty of care • Management of risk • Risk thresholds 	<p>PRESENTATION: Security & Programmes (35 mins)</p> <p>ACTIVITY: Risk Factors (10 mins) – global security challenges discussion.</p>	<ul style="list-style-type: none"> • S.2 Security & Programmes Session Plan • S.2 Security & Programmes Presentation
3	Security Risk Management	45 mins	<ul style="list-style-type: none"> • Security risk management • SRM framework • Policy, procedures and requirements • Role and responsibilities • SRM planning process • Resources & tools 	<p>PRESENTATION: Security Risk Management (30 mins)</p> <p>ACTIVITY: Essential Steps (15 mins) – SRM planning process exercise.</p>	<ul style="list-style-type: none"> • S.3 Security Risk Management Session Plan • S.3 Security Risk Management Presentation
4	Context Analysis	60 mins	<ul style="list-style-type: none"> • Analysing the operating environment • Incident monitoring • Mapping security stakeholders • Acceptance analysis • Sources of information 	<p>ACTIVITY: Visualising the Context (10 mins) – simple contextual factors exercise.</p> <p>PRESENTATION: Context Analysis (20 mins)</p> <p>ACTIVITY: Actor Mapping (30 mins) – security stakeholder mapping exercise.</p>	<ul style="list-style-type: none"> • S.4 Context Analysis Session Plan • S.4 Context Analysis Presentation
5	Risk Assessments	60 mins	<ul style="list-style-type: none"> • Risk assessment steps • Identify and evaluate threats • Determine risk • Risk treatment • Documenting risk assessments 	<p>PRESENTATION: Risk Assessment (30 mins)</p> <p>ACTIVITY: Risk Analysis (30 mins) – risk analysis matrix exercise.</p>	<ul style="list-style-type: none"> • S.5 Risk Assessments Session Plan • S.5 Risk Assessments Presentation

No.	Session	Time	Topics	Suggested Activities	Resources
6	Security Strategies & Approaches	45 mins	<ul style="list-style-type: none"> • Acceptance, protection and deterrence • Acceptance-based approach 	<p>PRESENTATION: Security Strategies & Approaches (15 mins)</p> <p>ACTIVITY: The Debate (30 mins) – security strategy debating exercise.</p>	<ul style="list-style-type: none"> • S.6 Security Strategies & Approaches Session Plan • S.6 Security Strategies & Approaches Presentation
7	Inclusive Security	45 mins	<ul style="list-style-type: none"> • Diverse staff profiles and risks • Inclusive security • Security management considerations 	<p>PRESENTATION: : Inclusive Security (25 mins)</p> <p>ACTIVITY: Diverse Profile Risks (20 mins) – risk exposure exercise.</p>	<ul style="list-style-type: none"> • S.7 Inclusive Security Session Plan • S.7 Diverse Profile Risks – Character Profiles • S.7 Inclusive Security Presentation
8	Security Planning & Plans	30 mins	<ul style="list-style-type: none"> • Developing security plans • SOPs and contingency plans • Security levels • Implementing security plans 	<p>PRESENTATION: Security Planning & Plans</p>	<ul style="list-style-type: none"> • S.8 Security Planning & Plans Session Plan • S.8 Security Planning & Plans Presentation
9	Managing Site Security	60 mins	<ul style="list-style-type: none"> • Site selection • Site protection measures • Image and acceptance • Managing guards 	<p>PRESENTATION: Site Security & Safety (40 mins)</p> <p>ACTIVITY: Field Office Assessment (25 mins) – site security exercise.</p>	<ul style="list-style-type: none"> • S.9 Managing Site Security Session Plan • S.9 Managing Site Security Presentation • S.9 Project Office Info Sheet
10	Managing Travel & Movements	60 mins	<ul style="list-style-type: none"> • Travel (road, air and other) risks • Field travel planning • Movement monitoring and communications • Air safety • Boat safety 	<p>PRESENTATION: Managing Travel & Movements (30 mins)</p> <p>ACTIVITY: Field Mission (30 mins) – journey planning exercise.</p>	<ul style="list-style-type: none"> • S.10 Managing Travel & Movements Session Plan • S.10 Managing Travel & Movements Presentation
11	Security Orientations & Briefings	30 mins	<ul style="list-style-type: none"> • Raising awareness • Staff security orientations • Visitor security briefings 	<p>ACTIVITY: Checklist (20 mins) – security orientation/visitor briefing checklist exercise.</p> <p>PRESENTATION: Security Orientations & Briefings (10 mins)</p>	<ul style="list-style-type: none"> • S.11 Security Orientations & Briefings Session Plan • S.11 Security Orientations & Briefings Presentation
12	Funding Security	30 mins	<ul style="list-style-type: none"> • Budgeting and resourcing for security 	<p>ACTIVITY: Costing Security (10 mins) – security risk management expenses exercise.</p> <p>PRESENTATION: Funding Security (20 mins)</p>	<ul style="list-style-type: none"> • S.12 Funding Security Session Plan • S.12 Funding Security Presentation

No.	Session	Time	Topics	Suggested Activities	Resources
13	Contingency Planning	60 mins	<ul style="list-style-type: none"> • Contingency plans • Hibernation, relocation and evacuation • When and who to withdraw • Basic preparations • Medical emergencies 	<p>ACTIVITY: Deteriorating Situation! (25 mins) – contingency planning exercise.</p> <p>PRESENTATION: Contingency Planning (35 mins)</p>	<ul style="list-style-type: none"> • S.13 Contingency Planning Session Plan • S.13 Contingency Planning Presentation • S.13 Deteriorating Situation! Handout
14	Incident Information Management	45 mins	<ul style="list-style-type: none"> • Managing incident information • Under-reporting • Immediate response • Lessons learned • Understanding the operating context • Strategic decision-making 	<p>PRESENTATION: Incident Information Management</p>	<ul style="list-style-type: none"> • S.14 Incident Information Management Session Plan • S.14 Incident Information Management Presentation
15	Critical Incident Management	135 mins	<ul style="list-style-type: none"> • Structure and responsibilities • Incident management plans • Critical incident response • Family support • Managing communications • Post-incident and after action review 	<p>PRESENTATION: Critical Incident Management (55 mins)</p> <p>ACTIVITY: Immediate Response Exercise (80 mins) – scenario-based exercise.</p>	<ul style="list-style-type: none"> • S.15 Critical Incident Management Session Plan • S.15 Immediate Response Exercise – Facilitator Brief • S.15 Immediate Response Exercise – Scenarios • S.15 Critical Incident Management Presentation
16	Security Collaboration & Networks	30 mins	<ul style="list-style-type: none"> • Inter-agency security networks • Saving lives together (SLT) • Partnerships and working with others 	<p>PRESENTATION: Security Collaboration & Networks</p>	<ul style="list-style-type: none"> • S.16 Security Collaboration & Networks Session Plan • S.16 Security Collaboration & Networks Presentation
17	Wrap-up & Evaluation	30 mins	<ul style="list-style-type: none"> • Participant Q&A • Parked topics/issues • Review expectations • Evaluation 	<p>Plenary Discussion</p>	<ul style="list-style-type: none"> • S.17 Wrap-up & Evaluation Session Plan • S.17 Training Evaluation Template

3. Training resources

Basic Security & Safety Awareness

- [Basic Security & Safety Awareness Session Plan](#)
- [Basic Security & Safety Awareness Presentation](#)

Personal Security & Safety

- [Personal Security & Safety Course – Sample Agenda](#)
- [S.1 Introduction Session Plan](#)
- [S.1 Introduction Presentation](#)
- [S.2 Threats & Risks Session Plan](#)
- [S.2 Threats & Risks Presentation](#)
- [S.3 Security Culture & Approach Session Plan](#)
- [S.3 Security Culture & Approach Presentation](#)
- [S.3 Policy – Fact or Fiction? Statement Sheet](#)
- [S.4 Shared Responsibilities Session Plan](#)
- [S.5 Inclusive Security Session Plan](#)
- [S.5 Diversity Iceberg Sheet](#)
- [S.5 In Someone Else's Shoes – Character Profiles](#)
- [S.5 Inclusive Security Presentation](#)
- [S.6 Personal Awareness & Behaviour Session Plan](#)
- [S.7 Site Security & Safety Session Plan](#)

- [S.7 Site Security & Safety Presentation](#)
- [S.8 Staff Travel & Movements Session Plan](#)
- [S.8 Staff Travel & Movements Presentation](#)
- [S.9 Information Security Session Plan](#)
- [S.9 Information Security Presentation](#)
- [S.10 Dealing with Incidents Session Plan](#)
- [S.10 Dealing with Incidents Presentation](#)
- [S.11 Incident Reporting & Support Session Plan](#)
- [S.11 Incident Reporting & Support Presentation](#)
- [S.12 Wrap-up & Review Session Plan](#)

Security Risk Management

- [Security Risk Management Course – Sample Agenda](#)
- [S.1 Introduction Session Plan](#)
- [S.1 Introduction Presentation](#)
- [S.2 Security & Programmes Session Plan](#)
- [S.2 Security & Programmes Presentation](#)
- [S.3 Security Risk Management Session Plan](#)
- [S.3 Security Risk Management Presentation](#)
- [S.4 Context Analysis Session Plan](#)
- [S.4 Context Analysis Presentation](#)
- [S.5 Risk Assessments Session Plan](#)
- [S.5 Risk Assessments Presentation](#)
- [S.6 Security Strategies & Approaches Session Plan](#)
- [S.6 Security Strategies & Approaches Presentation](#)
- [S.7 Inclusive Security Session Plan](#)
- [S.7 Diverse Profile Risks – Character Profiles](#)
- [S.7 Inclusive Security Presentation](#)
- [S.8 Security Planning & Plans Session Plan](#)
- [S.8 Security Planning & Plans Presentation](#)
- [S.9 Managing Site Security Session Plan](#)
- [S.9 Managing Site Security Presentation](#)
- [S.9 Project Office Info Sheet](#)
- [S.10 Managing Travel & Movements Session Plan](#)
- [S.10 Managing Travel & Movements Presentation](#)

- [S.11 Security Orientations & Briefings Session Plan](#)
- [S.11 Security Orientations & Briefings Presentation](#)
- [S.12 Funding Security Session Plan](#)
- [S.12 Funding Security Presentation](#)
- [S.13 Contingency Planning Session Plan](#)
- [S.13 Contingency Planning Presentation](#)
- [S.13 Deteriorating Situation! Handout](#)
- [S.14 Incident Information Management Session Plan](#)
- [S.14 Incident Information Management Presentation](#)
- [S.15 Critical Incident Management Session Plan](#)
- [S.15 Immediate Response Exercise – Facilitator Brief](#)
- [S.15 Immediate Response Exercise – Scenarios](#)
- [S.15 Critical Incident Management Presentation](#)
- [S.16 Security Collaboration & Networks Session Plan](#)
- [S.16 Security Collaboration & Networks Presentation](#)
- [S.17 Wrap-up & Evaluation Session Plan](#)
- [S.17 Training Evaluation Template](#)