The following document has been prepared by the ACT Alliance Safety & Security Community of Practice (SSCP) for use by ACT Alliance members and partner organizations. This document can be found, along with other ACT safety and security tools on the SSCP website: www.act-security.org
# ACT Security Focal Point Manual

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to use this manual: Purposes and Objectives</td>
<td>2</td>
</tr>
<tr>
<td>Overview of the Security Focal Point (duty of care)</td>
<td>2</td>
</tr>
<tr>
<td>ACT Alliance Joint Security Focal Points</td>
<td>4</td>
</tr>
<tr>
<td>SFP Percentage of Role <em>(linked to country risk rating)</em></td>
<td>6</td>
</tr>
<tr>
<td>Responsibilities of an SFP</td>
<td>7</td>
</tr>
<tr>
<td>Context Analysis and Risk Assessment</td>
<td>10</td>
</tr>
<tr>
<td>Security documents</td>
<td>12</td>
</tr>
<tr>
<td>Local security coordination</td>
<td>14</td>
</tr>
<tr>
<td>Gender and disability security</td>
<td>15</td>
</tr>
<tr>
<td>Incident mapping and reporting</td>
<td>15</td>
</tr>
<tr>
<td>Annex A: Job Description of an internal SFP</td>
<td>19</td>
</tr>
<tr>
<td>Annex B: Job description of a shared ACT SFP</td>
<td>21</td>
</tr>
<tr>
<td>Annex C: ACT Security Risk Assessment Tool</td>
<td>23</td>
</tr>
</tbody>
</table>
1. How to Use This Manual

- Purpose and objectives
- Scope of SFP roles
- This manual and SFP training

This document was prepared by the ACT Alliance Safety & Security Community of Practice (SSCP) to provide adapting guidance for existing or new Security Focal Points (SFPs) working in different ACT Alliance members organizations or partner organizations and provide recommendations for an SFP training package. This document can be used by both international and national organizations working in the fields of humanitarian assistance, sustainable development and advocacy/human rights.

1.1 The scope of SFP roles will vary from organization to organization but the essential functions remain common across all types of ACT members. In reading and utilizing this document, it is strongly recommended to take into account the security context/environment(s) in which the organization operates, the types of programs you have and the way in which you work (direct implementation, working through local partners or other methodologies).

1.2 This document has been designed to be used in conjunction with a one-day SFP training course. The SSCP can schedule SFP training alongside ACT Security Courses, which are delivered in global regions annually. While all ACT staff should attend a security course, the SFP training is focused on the SFP within the organization. This can include those with responsibility at the international HQ level, national level or those responsible for specific locations within a country.

For information on where and when SSCP training will take place, see their website: www.act-security.org

2. Overview of the Security Focal Point

- Purpose of the SFP role
- SFP responsibilities
- Duty of Care
- Developing staff awareness
- Who can be an SFP?

All organizations should have a security focal point. It would be naïve as well as a legal and moral failure for both national and international aid organizations to not recognize the increasing risks faced by aid workers; including faith-based organizations. Most international NGOs will have a full time or part time senior SFP at the headquarters level and also at the country office level. National NGOs usually have one staff
member designated as a part time SFP within the office. Field offices may also have designated SFPs responsible for their local areas.

2.1 Aid organizations can address safety and security issues through the use of security managers, security advisors or SFPs. For the purposes of this document, these can be defined as:

**Security Managers:** A staff role that has a decision-making capability within their job description and may line or matrix-manage staff with a security function within the organization, including SFPs.

**Security Advisors:** A staff role or consultant who provides safety and security advice to management and staff but normally has no decision-making authority.

**Security Focal Points:** A staff role at the HQ, national or local level that is often a secondary duty as part of the individual’s job description.

The purpose of the SFP role is to give one (or more) persons direct or delegated responsibility for security risk management within the organization. This can include the following roles and responsibilities:

- Maintaining the security plan and other security documents including regular reviews of the threat environment and making changes/adaptations to the security plan’s Stand Operating Procedures (SOPs).
- Conducting risk assessments, or ensuring they are done, as part of planning travel, hosting meetings and as part of programme activity.
- Providing security briefings and cultural awareness information to international visitors and new staff as part of their induction.
- Attending security coordination meetings with local forums, UN agencies or other safety and security networks in their context and sharing relevant information with their management and staff.
- Organizing training for staff in personal security, first aid and other safety subjects (safe driving, dealing with aggression, gender security, fire safety…)
- Conduct or analyse investigations when incidents occur and report results to management for follow up with recommendations for changes to improve safety and security.
- Liaising with other SFPs, especially ACT members, in your context around common threats and effective coordination to reduce risk levels.
- Holding fire evacuation drills periodically.
- Ensuring emergency phone trees are kept up to date.
- Advising the crisis management team in the event of a crisis.
- Ensuring office security policies and access control systems are adhered to.
2.2 The concept of ‘Duty of Care’ has become increasingly important for aid organizations in recent years. NGO’s have a legal and moral responsibility to take all reasonable actions to ensure their staff are safe, and not put them in harm’s way without their knowledge (informed consent). The UN, most major donors, Core Humanitarian Standards (CHS) structures and many government legal codes require aid organizations to have clear duty of care policies. The SFP’s have a key role in ensuring that both staff and management understand their security responsibilities and make staff safety a cornerstone of any activities undertaken by the organization.

2.3 It is important to note that one challenge for the SFP is convincing staff that while they may be comfortable in accepting risk personally, the organization has a duty to protect itself, its staff and its reputation. If a staff member is injured or killed, that is always a tragedy, but the organization may face angry family members, demands for compensation, legal charges and damage to reputation in the community, with the host government, with donors and other staff. It may even affect the organizations ability to continue working, which affects livelihoods of beneficiary communities. So getting staff to understand that security risk management is a priority can be critical to success.

2.4 Staff designated as SFP’s are rarely security experts. They are normally HR staff, admin staff, programme staff or someone who has demonstrated the skill or aptitude for managing this portfolio. While retired soldiers or police do sometimes take these roles, it is not a requirement. Often it can pose a challenge as former security force personnel can have difficulty understanding an aid organization’s perception of risk, our code of conduct and especially how we address our concerns…i.e. without guns, armoured vehicles or barricades. Many SFPs at a senior headquarters level started as programme staff who took a serious interest in security issues and followed that career path. So a background in security is not always a prerequisite for being a successful SFP.

3. ACT Alliance Joint Security Focal Points

- Role of joint ACT SFPs
- Responsibilities of a joint SFP in emergencies

In several regions globally, ACT National Forums in insecure contexts have combined resources to hire a joint SFP. This has been done to better respond during natural disasters and during conflict/man-made disasters. The SFP role is normally hosted by one of the ACT members although the SFP provides support to all members in that country or region.

3.1 Joint ACT Alliance security focal points can be helpful when ACT members respond to large, rapid onset emergencies where large numbers of ACT members deploy staff to a region that does not have enough local security capacity to manage
the response initially. In these circumstances, joint SFPs will have the following responsibilities:

- Deploy in the ‘first wave’ and conduct a rapid security risk assessment ahead of the majority of staff arriving. This would include:
  - Immigration concerns and challenges around international staff or equipment
  - Safe and adequate accommodations
  - Safe and adequate access to safe drinking water and food
  - Reliable communications (internet and phone)
  - Access to medical care locally and location of insurance-approved in-country medical facilities
  - Assess attitudes of local communities to the arrival of foreign aid workers
  - Cultural norms that need to be respected
  - Legal representation in the event of an incident or arrest of staff
  - Gender security issues including LGBTI staff deploying
  - Establishing links to local security forums or other NGO SFPs
  - Establishing links with UNDSS or other UN Security agencies or NGO security networks if present
  - Meeting with embassy staff representing arriving aid workers (if present) to confirm contact points and support available

- Integrate the security risk assessment into the initial needs assessment for program design and response planning.
- Develop and provide a security briefing for all arriving personnel and for new national staff.
- Establish a phone tree for use in emergencies
- Contact ACT member crisis management teams and have clarity on how to interact with the SFP in event of a security crisis situation.
- Develop training plans for national ACT member staff on safety and security and ensure responding members budget for this.
- Ensure as many staff as possible receive adequate first aid training and first aid kits are made available.
- If a joint ACT compound is used, ensure the compound meets the ACT guidelines on security standards for shared ACT facilities. These are available on the SSCP website, www.act-security.org http://www.act-security.org/download/Shared_Facilities_Minimum_Standards_Guidelines.pdf
- Represent ACT members at local security meetings.
- Maintain an incident map of any security incident affecting any NGO in the context.
- Provide advice to ACT member management teams on security issues.
- Prepare weekly and monthly reports on the security situation to be distributed to the active or supporting members.
- Investigate or analyse incidents and make recommendations to improve SOPs to prevent further incidents.
- Support programme staff in developing risk assessments for ACT appeals or other project proposals. Ensure adequate funding for security costs is included in programme funding plans.

4. **SFP Percentage of Role**

   - Country Risk Ratings and SFPs
   - Percentage of time an SFP should have in their role
   - HQ SFPs

   There is no set standard for the percentage of time a staff member designated as an SFP should dedicate to this role. However, the SSCP advises that the role be linked to the country risk rating system. These are:

   - **Country Risk Rating 1: Very Low Risk** (Peaceful states, minimal crime, no regular natural disasters)
   - **Country Risk Rating 2: Low Risk** (No armed conflict, low crime, some natural hazards)
   - **Country Risk Rating 3: Moderate Risk** (Some armed violence/conflict, crime more common, natural hazards present)
   - **Country Risk Rating 4: High Risk** (Regular armed violence/terrorism, high crime rates, regular natural disasters)
   - **Country Risk Rating 5: Very High Risk** (Open state of war, NGOs targeted, crime a daily occurrence, ongoing natural disaster)

   *(Note: The SSCP has an ACT country risk rating table. Members can contact the ACT Security Coordinator for the risk rating of any country ACT members are currently active in)*

   4.1 Based on the above, a baseline for considering the percentage of time a staff position should be dedicated to the SFP role could be recommended as follows:

   - **Country risk rating 1:** 5-10% of role/time
   - **Country risk rating 2:** 10-20% of role/time
   - **Country risk rating 3:** 20-50% of role/time
   - **Country risk rating 4:** 50-75% of role/time
   - **Country risk rating 5:** 100% of role/time
4.2 For headquarters SFP’s the same formula can be used depending on what the typical country risk ratings are for the areas where the organization operates globally.

5. Responsibilities of an SFP

- Prioritizing security in NGO daily life
- Accept responsibility that advice can affect lives
- Dealing with the ‘boiling frog’
- Challenges in faith-based organizations
- Organize training and keep records of staff qualifications

In the normal routine of an aid organization, the constant cycle of designing new programmes, securing funding, delivering projects and reporting to donors can make it difficult for ‘lesser’ priorities to gain acceptance. Very often, before any major security incident occurs, many NGO’s just do not prioritize staff safety and security. Therefore, it is a major responsibility of the SFP, with backing from management, to advocate for security to be integral to everything the organization does, from hiring new staff (background checks, code of conduct training), to programme design (what threats will the project face and how do we mitigate the risks), and even social media policies (how to protect staff identities and activities in challenging contexts). Essentially, every department of an NGO has a role to play in security and duty of care.

Senior management:
- Establishing and enforcing security policies
- Sourcing funding for staff security training, equipment
- Preparing crisis management plans
- Ensuring reputation risk issues are dealt with effectively

Admin/HR Staff
- Ensuring facilities have proper security features
- Adequate security for records/contracts/personnel documents
- Background checks on new staff
- IT security for office servers
- Emergency supplies procured and accounted for
- Regular fire inspections and fire extinguishers
- First aid kits in vehicles and in key office locations
- Legal compliance with labour codes

Finance Staff
- Secure storage/transit of cash
- Security of financial records
- Payroll security
- Ant-fraud and anti-corruption practices
- Access to emergency funds in event of crisis

Programme Staff
- Security risk assessments as part of programme design
- Building acceptance in targeted communities
- Ensuring project staff provided with safe vehicles, security training, first aid kits, reliable communications
- Ensuring anti-fraud and anti-corruptions protocols followed
- Reporting, investigating and analysing security incidents to learn lesson and improve procedures
- Coordination with other NGO’s, government departments, UN agencies, donors on safety and security issues in program locations

Drivers/Logistics
- Ensure major assets like vehicles are well maintained
- Vehicles properly equipped for the types of work they do
- All assets are secured from theft or vandalism
- Procurement policies are followed to prevent fraud or loss due to scams or mismanagement
- Travel safety policies are known and enforced

5.1 It is the SFP’s role to ensure each department understands their security responsibilities and takes appropriate measures to ensure they do not fail in their duty of care.

5.2 Accepting Responsibility

One factor that is often overlooked, but can have serious consequences, is that while each individual must accept responsibility for their own security choices, both management and individual staff will rely on the advice of the SFP to make those choices. In selecting an appointing an SFP management must select those who have the moral strength to assess risk impartially and give their best advice. Some SFPs (and organizations) develop a very risk averse mind set and that prevents aid projects that could proceed to be delayed over a fear of possible consequences. Others may underplay risk levels so that they do not lose funding through delays or poor monitoring. SFPs must be able to balance these competing views and provide their best advice to management to staff safe while also allowing programming to continue.

5.3 The Boiling Frog
This expression has been used by SFPs for many years and refers to the folk story that a frog thrust into boiling water will immediately jump out; but if the frog is put in cool water and the heat starts to rise, it will keep swimming and hoping things will be better soon until it boils to death. The lesson here is people who stay in a high threat environment too long, or disregard a worsening situation and hoping life will improve soon, risk becoming a boiling frog.

5.3.1 The SFP must be able to take a step back and look at the situation the way an outsider or international HQ would. This effort is helped if incident records are kept that can give evidence to show when a situation is deteriorating (increased crime, more terrorism incidents, rising water levels in flood-prone areas etc.).

5.4 Challenges in Faith Based Organizations

While most modern, faith-based organizations will be practical and realistic about threats faced by staff, some do still rely on faith for their security. While this is admirable and certainly helps staff cope with the threats they face, as an organization this attitude can be a source of increased risk.

5.4.1 Any individual can choose to undertake a mission, deployment or field trip because their faith gives them the courage to do so. But an organization cannot make that choice for the individual. So if an international headquarters or country office develops a project that requires staff to travel to at-risk locations to deliver the aid, they have a legal and moral responsibility to take all reasonable measures to ensure the safety of the staff. Relying on faith alone will not comfort surviving family members if staff are killed or seriously injured when more practical measures could have been taken.

5.4.2 There has been a long debate as to whether faith-based or secular aid organizations are most at risk in the modern context. There have been studies done, including an excellent one by the European Inter-Agency Security Forum (EISF):


The consensus is that it depends on the risk assessment and local context. Generally in conservative cultures with strong faith elements, expressing no religion is far more suspicious than working for an organization from a different faith. Do not necessarily assume that Muslim, Hindu, Buddhist or other communities will automatically be suspicious of Christian organizations or vice versa. As long as the organization does not proselytize as part of their engagement with the community there is often little additional risk. But a proper context analysis and risk assessment will highlight these concerns.
5.5 Organize Training

It is the role of the SFP, in cooperation with management, to organize or facilitate the process of security training for staff. This can include:

- Online security induction training (see the SSCP online course on our website: [www.act-security.org](http://www.act-security.org))
- Two or three day security trainings covering personal security, security mitigation for local threats and security risk management techniques.
- First aid training
- Driver training
- Crisis management training
- Gender security training

5.5.1 All of these are available from the ACT SSCP. They are also often available through local security forums, UN agencies and commercial companies.

5.5.2 The SFP should also keep records of who in the organization has completed the various security trainings and ensure refreshers are scheduled every 1-3 years depending on the security context(s) where the organization operates.

6. Context Analysis and Risk Assessment

- The Security Context Analysis
- The Security Risk Assessment

Two of the key tools of an SFP are the security context analysis and the security risk assessment. In order to work effectively and efficiently in any context, the information these tools provide needs to be identified and regularly updated.

The Security Context Analysis

This is a process where the SFP and supporting staff (senior management, programme staff, possibly implementing partners) examine key stakeholders in a country or programming region that may impact the security context in a positive or negative way. This stakeholder analysis should provide insight into the motivations, mandate or specific interests of each and how interacting with one may influence relations with others. These stakeholders can be government departments, traditional leaders, UN agencies, other NGOs, business communities but also criminal gangs/rebel groups active in the operational area.
6.1 To conduct a security context analysis, list all the stakeholders, formal and informal. For each actor, identify what role they play in the context, how they influence the context, the way the stakeholder interacts (positively or negatively) and how your organization will need to engage with these actors or maintain awareness of each. Finally, assess how each stakeholder can influence your acceptance strategy in the country and with the communities you work with.

6.2 While the security context analysis is a valuable tool for international agencies who are new actors in a context, the analysis is also valuable for national organizations to reflect and assess their inter-relationships with the different actors involved. This is a key method of avoiding the 'boiling frog' syndrome.

The Security Risk Assessment

The risk assessment is a key tool for an SFP. Through proper risk assessments your organization and staff are informed about the challenges they may face in their work and recommends mitigation strategies to reduce the chance of an incident or limit the damage if one does occur. Risk assessments should be conducted for:

- The overall country context (in conjunction with your security context analysis)
- The environment where your organization will implement or support programs delivered through other implementing partners
- As part of the initial stages of any program proposal/development/design
- Ahead of any major workshop, conference or high profile visitor(s) arrival
- Around specific gender issues related to threat to men, women and LGBTI in your context
- As part of any travel to category 3/4/5 risk areas (moderate/high/very high risk)
- When staff, the organization’s reputation or other situations may put people at risk based on an activity conducted by your NGO, such as cash-based programming, human rights advocacy or in complex religious, ethnic or political environments.

6.3 There are a number of guides and templates available for conducting security risk assessments on the SSCP website: [www.act-security.org](http://www.act-security.org). These include:

- ACT Alliance Security Risk Assessment Tool (See Annex C)
- Hotel Security Risk Assessment Form

7. **Security Documents**

- Security policy
- Security plans
- Crisis management plan
- Contingency plans
- Security briefings

All organizations should have a series of security-related documents. Some organizations make the mistake of trying to cram all their information into one large document. Generally, any document over 25 pages will never be read and few staff will be able to recall the content specifics. It is always advisable to have a series of short documents that meet each need. These documents below are key documents that are in addition to the context analysis and security risk assessment.

**The Security Policy**

This is a management document that lays out the organization’s priorities, principles, responsibilities and systems to be used to meet their responsibility for Duty of Care. This document should reflect the Code of Conduct and establish how security will be managed within the organization.

**The Security Plan**

This document is for all staff to read and understand as it informs them of the threats they face and how to reduce their exposure to each. This document should include short summaries of the security policy, context analysis and risk assessment. The main body of the security plan should be short, clear guidance for staff to minimize their vulnerability to ALL threats identified in the risk assessment. A good checklist for a security plan is available from the SSCP website [www.act-security.org](http://www.act-security.org). The ACT Safety & Security Guidelines can also provide a good basis for a security plan.
Crisis Management Plan

Again, this is a management document that outlines how the organization will manage a serious, extended crisis. It should identify who is on the CM team, who has decision-making authority (especially between HQ, regional and country offices) and what the priorities are. Further information on crisis management can be found in the EISF resource library at www.eisf.eu

Contingency Plans

In the security context, contingency plans are designed to give guidance to the crisis management team in the event a crisis occurs. These can be prepared for major events that were identified in your security risk assessment. Some typical contingency plans are:

- Hibernation, relocation, evacuation
- Natural disaster (earthquake, flood, hurricane, volcanic eruption or other)
- Kidnapping, abduction or arrest
- Armed conflict
- Election periods (before, during and after)

Note: Contingency plans for the SFP are not about programming! The aim of safety and security contingency plans are to save staff lives, protect major assets (offices, vehicles, equipment) and protect the reputation of the organization with different stakeholders and the public. The organization has to survive before it can assist anyone else. Often programme staff want to leap into emergency response work before staff safety can be assured. A template for contingency plans is available from the SSCP website: www.act-security.org

Security Briefing

It is important to have a security briefing prepared for any international visitors or new national staff moving from one internal context to a new context. This should include:

- An overview of the country and program locations/type of programs
- A summary of the risk assessment
- The social and cultural habits locally to ensure visitors understand the norms and taboos.
- Basic maps of office locations and information on safe travel between the airport, hotels and offices
- Information on health risks, immunizations required and medical service in country
- Visa information (costs, how to access, types of visas needed)
➢ Emergency contact numbers
➢ Places, locations, neighbourhoods to avoid

These briefings can be adapted for hosting conferences or workshops. Or for other activities where visitors are going to be present.

8. Local Security Coordination

➢ NGO Forums
➢ Other sources of information

In most contexts there will be some form of NGO forum where national and international aid organizations coordinate and discuss safety and security challenges. In regions with higher levels of security risk, these forums may often have security on the agenda. In high risk locations, a separate NGO security forum may be organized for SFPs to share information, training costs and other support initiatives.

8.1 The SFP has two responsibilities in relation to NGO forums:

➢ To attend these forums and actively contribute in providing security information, incident information (sanitized) and lessons learned
➢ To take new information back and disseminate to relevant staff so that all important information is shared and measures taken accordingly

8.2 Other sources of information within most contexts can include:

• UN agencies including UN Department of Safety & Security (UNDSS)
• National government (including police and military advisories)
• Major donor representatives
• Insurance company information services
• Community structures
• Security guard companies
• Embassies if you have international staff
• International NGO Security Organization (INSO) if an office is present
• Local partner organizations
• United States Geographical Service (USGS) for earthquake warnings
• Meteorological services for extreme weather warnings

8.3 The SFP is responsible for establishing contacts with as many sources of information as possible. They will need to regularly check/verify or discount rumours when there are indications of increased levels of threat or other risks that can affect the organization and staff safety.
9. Gender and Disability Security

- Different threats faced by each gender
- Considering national and international gender concerns
- Security challenges facing disabled staff

While all staff may face threats in the conduct of their work, it is often the case that each gender can experience the risks differently. For example:

- Men may face increased suspicion by security forces, be culturally forced to take risks and face peer pressure to demonstrate their 'manhood.'
- Women are often more likely targets for crime as they are perceived as less of a risk for fighting back, more likely to be sexually harassed or face sexual violence/assault.
- Lesbian, Gay, Bisexual, Transgender and Intersexed (LGBTI) staff often face discrimination, violence, arrest and reduced access to benefits or medical support.

9.1 The SFP will need to take these issues into special consideration for both national and international staff (including visiting HQ representatives, consultants or volunteers). The context analysis and security risk assessment must include gender issues and provide advice to all staff on how to minimize their risk to threats present to each gender in the context.

9.2 The SSCP has a gender security handbook which is available on the SSCP website (as of December 2016). They also conduct one-day gender security trainings in each global region annually.

9.3 Staff with disabilities may also face increased safety and security challenges including harassment, safe access, ability to evacuate a building during a fire or safe transport options to and from their place of work.

10. Incident Mapping and Reporting

- Incident mapping as an effective tool
- Other uses of mapping
- Incident reporting and sharing

On a daily and week-by-week level, incident mapping can be one of the most effective tools of the SFP to monitor the security situation, but also to see if risk reduction measures need to be changed.
By noting where incidents occur, who was targeted, what time of day, identity and motivations of the attacker(s) and any other relevant information, the SFP can better monitor trends in the operating context.

10.1 By making optimal use of the incident analysis the SFP can adapt Standard Operating Procedures (SOPs) to assist staff to avoid danger areas during at-risk time periods or avoid certain routes where incidents most often occur. The incident map also serves as the evidence that the SFP needs to have in order to convince staff and management that the situation is changing and changes to security measures are needed. This is also a process for learning lessons, avoiding repetition of incidents and avoid the 'boiling frog' syndrome.

10.2 Effective communication equipment for safety and security is key at all times and therefore staff need to know which areas have adequate mobile coverage and which areas have weak or no signal. These areas can marked on a separate map or overlay so staff can plan their travel to avoid areas with poor communication options or plan to use alternative means of communications such as satphones, radios or...
tracking systems. Staff can also plan check-in times before entering dead zones and after exiting to confirm safety during travel.

10.3 Other security information that could be included on incident maps to increase staff safety:

- Locations of other NGO offices where staff could seek assistance
- Locations of hospitals, clinics or other medical support
- Locations of police stations
- Locations of guest houses, fuel stations or shops that staff may need to access.
- Any other information that may assist staff in staying safe while away from the office.

10.4 Reporting

An SFP can make use of information from many sources to fill out their incident map. This often includes information from other NGOs in your context. The situation works both ways however and the SFP will be expected to share information on incidents affecting their staff with other organizations; either within the NGO forum, other trusted security network and their HQs.

10.5 Many organizations have an incident reporting form. If not, the essentials always remain the same:

- Who was involved?
- Where did the incident occur?
- What times did events occur?
- What happened?
- What actions were taken?
- Any deaths, injuries, losses or damages?
- Who was informed (police, hospital, insurance, family, line manager, other)?
- Any recommendations to avoid a similar incident in the future?

10.6 It is strongly advisable to have those involved record their thoughts as soon as possible after an incident, when the memory is most clear and details remain fresh.

10.7 ‘Sanitized’ summaries of the incident reports (no names, exact locations), can be shared externally to increase security awareness and learning by partner organizations and other NGOs.

10.8 The objective of incident reports is to learn from each and be able to adapt SOPs to prevent further incidents. But also, if there were ever questions by family
members, police, insurance providers, donors etc., the incident report becomes the key reference document.
Annex A: Job Description of an Internal Security Focal Point

Objective:
Provide safety & security advice and support to the (location) management team and staff.

Reporting to:
(The SFP should report to the senior management team at HQ, regional or national level).

SFP Role and tasks

Safety & Security information

- Conduct risk assessment and context analysis as needed to inform on security strategies.
- Short term: gather & disseminate day to day safety & security related info
- Longer term: gather & disseminate weekly/monthly/quarterly/annual developments to Country Rep, LWF staff etc.
- Networking with UN (OCHA, UNDSS), ACT Alliance, NGO security networks (e.g. INSO), others.

Providing info & operational security support

- Security briefing to new staff, visitors and consultants
- Develop & maintain a security briefing that includes local safety & security conditions
- Provide regular (verbal) updates and advice during team meetings
- Prepare written security updates upon request
- Organize/provide discussions, workshops, training etc. for staff
- Monitoring of agreed security procedures & remind staff on maintaining them
- Ensure that security is included in the set-up of (new) programs and budgets
- Organize/provide logistics & administrative support in the field of communication, transport, compound security.
- Ensure safety & security measures are implemented in the (insert location) office compound, fire prevention, evacuation procedures, office burglar proof, earthquake proof, etc.

Safety & security assessment & planning

- Prepare& keep updated the (HQ/Regional/Country) Security Plan (CSP) – at least annually.
- Facilitate application and practical organization related to safety & security related Standard Operational Procedures (SOPs) and Hibernation, Relocation and Evacuation plans (HRE plan)
- Make/organize security assessments of locations and travel possibilities.
Incident management support

- Provides follow-up in case of safety & security related incidents
- In case of serious incidents, inform and provide advice to senior management team.
- Complete or ensure incident report is completed and submitted to relevant management.

Overview of SFP stakeholders

- Senior management team
  Staff with specific security tasks such as guards, drivers
- Other ACT alliance members in (SPECIFIC COUNTRY) colleagues/staff members
- International/national NGOs
- UN security related contact persons
- Inter-NGO security chains/bodies
- Embassy contact persons
- Authorities: police, army, peace keeping forces, etc.

SFP profile-competencies-requirements

- Is accessible on a 24/7 basis for urgent security related issues.
- Having knowledge on NGO security issues, skills to analyze and solve security issues, and an NGO security attitude (focus on the risk reduction strategies of ‘community acceptance’ and partly protection)
- Able to strike a balance between performing operational tasks and planning/policy preparation tasks.
- Creating and maintaining a relevant network for up-to-date and solid security information.
- Able to stimulate/train security alertness amongst management and colleagues.
- Creating and having the seniority to identify non-compliance to agreed procedures, non-constructive security related behavior, etc. and to provide feedback on this to colleagues and management.
- Able to react swiftly and effectively to security related incidents.
- Having successfully and recently attended a basic security course and preferably a SFP specific course.
Annex B: Job Description of a Shared Security Focal Point

Objective:

Provide safety & security support for staff and visitors related to ACT alliance members currently active in (insert location). The Security Focal Point will ensure that relevant and achievable safety/security protocols are established and maintained in order to provide safety and security services to the staff as well as safe delivery of relief/recovery materials to the intended communities.

Reporting to:

The Shared SFP Role will be matrix-managed and report primarily to the Chair of the ACT National Forum. The SFP will also report to the designated senior management role at the hosting ACT member.

SFP Roles and responsibilities

I. Gathering information

- Develop security risk assessments and context analysis to inform common security plans.
- Short term: day to day safety & security related
- Longer term: weekly/monthly/quarterly developments
- Networking with all ACT members in context, partner organizations, ACT Safety & Security Community of Practice (SSCP), UN, other NGO networks and host government security points as appropriate.

II. Providing info & operational security support

- Provide security briefing to all incoming ACT staff on security situation and recent developments
- Brief all ACT staff on safety and security situation a weekly / bi-weekly
- Write risk assessments for areas of operation
- Representing ACT alliance forum in security related networks
- Be POC (Point of Contact/recipiecnt (alternate Team Leader) for Field Trip Plans which should be delivered prior to trip commencement for authorization by team leader.
- Be POC for “Check- in Procedure” for expat staff in field
- Liaise with relevant forums to obtain up to date info on safe / unsafe roads
- Organize/provide discussions, workshops, training etc. for staff
- Remind staff on maintaining current/agreed procedures
- Organize/provide logistics & administrative support in the field of communication, transport, compound and warehouse security.

III. Safety & security assessment & planning
- Support and update a shared ACT security plan or support individual ACT members in developing their own security plans while ensuring compatibility within the forum.
- Facilitate practical organization-related to safety & security related Standard Operational Procedures (SOPs) and Contingency Plans (CPs)
- Make/organize security assessments of locations, travel possibilities, etc
- Establish office and accommodation security, including fire extinguishers and smoke detectors, First Aid kits, alarms, fire escapes etc.
- Provide list of shortcomings within 2 months according to minimum ACT standards for joint compounds (see SSCP website www.act-security.org)

IV Incident management support
- Provide operational support in case of safety & security related incidents
- Investigate safety & security incidents and report findings to Chair of ACT Forum while respecting confidentiality of those involved.
- Recommend improvements to policies, plans, SOPs to prevent similar incidents where possible.

V SFP stakeholders / network
- ACT Forum and member senior management teams
- ACT alliance staff with specific security tasks such as guards, drivers (hierarchical or functional management)
- Other ACT alliance staff members (advice, support, monitoring their behavior)
- Sharing security information with ACT SSCP (Safety and Security Community of Practice) via the ACT Global Security Advisor James.Davis@actalliance.org
- International/national NGOs (info and best practices exchange)
- Security related staff of Partner organizations (info and best practices exchange. Support?)
- UN security related contact persons (info, possibly evacuation support?)
- Inter- NGO security chains/bodies (info, exchange, training)
- Embassy contact persons (info, possibly evacuation support)
- Authorities: police, army, peace keeping forces, etc. (information sharing, in some countries: support)

Qualifications and competencies:
- Experience in providing security training and advice
- Experience in doing risk assessments
- Able and willing to frequently visit field locations
- Good communication and networking skills
- Relevant experience in context.
ANNEX C    ACT Security Risk Assessment Tool

1. Purpose of This Tool

Each ACT Alliance member has a Duty of Care for their staff, programmes, partners and communities in which it works. Meeting this duty requires members to ensure they do not knowingly, or negligently, place their people and projects in unsafe or insecure situations. To accomplish this goal, organizations must be able to critically assess threats and develop strategies to mitigate their exposure. This tool is designed to allow all ACT members to undertake a systematic evaluation of their exposure to threats and then develop strategies to reduce the risk. This can be valuable for both safety & security planning as well as programme funding proposals that require a risk assessment.

2. How to Use This Tool

The safety and security risk environment can cover a broad range of threats from violence, conflict, natural hazards, terrorism, health issues, political interference, crime or corruption. This tool is designed to allow ACT members without any specific security background to conduct a basic security risk assessment as part of any wider assessment process. If the result is an assessment of a high level of threat or a complex risk and threat environment, ACT members may choose to request additional security support through the ACT Rapid Support Team (RST) or alternatively, through the ACT Safety & Security Community of Practice (SSCP).

This Assessment Tool is broken down into three steps:

1) Identifying the risks
2) Evaluating and rating the risks
3) Methodologies for reducing or mitigating the risks

NOTE: It is important for all organizations to understand their ‘threshold’ for risk as both an organization and for their staff. Some organizations are experienced and trained to work in moderate to high risk environments while others may only have the capacity to work in low to moderate risk areas. It is important to know what your organizations’ ability to manage risk is in determining what your threshold should be for responding to an emergency.
1. Overview

There are many methodologies for identifying risks from actor mapping to complex context analysis. These are excellent tools and should be used whenever possible.

1.1Sources of information for your risk assessment can include:

- NGO forums
- Other ACT members
- Community groups
- INSO reports
- UNDSS reports
- Local and international media
- Insurance companies
- Host government agencies

1.2Another method is to gather staff together including management level representatives, admin staff, program staff, drivers and even security guards. Each group may feel they face different types of threats. List all the threats identified by the group.

1.3 Definitions

**THREAT:** Something that exists in the environment in which you live and work

**Risk:** Your exposure to that threat

2. Types of Risk

Below is a table of risks that you typically may face in responding to any rapid onset emergency or humanitarian disaster. Are any of these applicable in your response areas?

<table>
<thead>
<tr>
<th>Violent Threats</th>
<th>Organizational Threats</th>
<th>Environmental Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Targeted armed attack</td>
<td>• Reputation risk</td>
<td>• Natural hazards (weather, earthquakes, flooding, etc)</td>
</tr>
<tr>
<td>• Non-targeted armed conflict</td>
<td>• Financial risk (banking, currency exchange, theft, misappropriation)</td>
<td>• Medical risks (access to suitable medical treatment for staff)</td>
</tr>
<tr>
<td>• Kidnapping</td>
<td>• Corruption/Fraud</td>
<td>• Health issues (food, water, disease, rest)</td>
</tr>
<tr>
<td>• Terrorism</td>
<td>• Legal risk (work permits, local legal compliance, resistance to advocacy)</td>
<td>• Traffic accidents</td>
</tr>
<tr>
<td>• Landmines, IEDs, bombing</td>
<td>• Political risk</td>
<td>• Other accidents</td>
</tr>
<tr>
<td>• Carjacking</td>
<td>• Work place violence or discrimination</td>
<td>• Fire</td>
</tr>
<tr>
<td>• Sexual violence</td>
<td>• Cultural challenges to Code of Conduct</td>
<td>• Stress</td>
</tr>
<tr>
<td>• Civil unrest</td>
<td></td>
<td>• Other?</td>
</tr>
<tr>
<td>• Religious violence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Crime</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Other?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
List your Threats:

<table>
<thead>
<tr>
<th>The Threat</th>
<th>What Locations</th>
<th>Who/What will be at Risk?</th>
<th>What will the affect be?</th>
</tr>
</thead>
</table>
| List one threat identified in Step One | Is the threat confined to one or more areas or across the entire affected region? Be specific. | • International staff  
• National staff  
• Community members  
• Marked vehicles  
• Aid supplies  
• ?? | • Loss of life  
• Loss of assets  
• Damage to reputation in community/with gov’t  
• Reduction is ability to work |
| Complete for each threat identified in Step One | | | |

2. Rating the Risk

Once you have evaluated each risk and understand what challenge it represents to any emergency response activities, it is important to rate the risk. This clarifies for all individuals and organizations reading the report how severe (or not) the risk is and how much priority it must be given under the Duty of Care.
2.1 The risk rating is derived from a combination of the probability that an incident will occur and the level of impact it will cause. Most NGOs and the UN use a risk rating system similar to the following:

1. **Very Low**
2. **Low**
3. **Moderate**
4. **High**
5. **Very High**

2.2 Below is a table you can use to determine the risk rating for each threat you have identified.

**Risk Rating Table:** Apply to each threat identified.

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IMPACT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Very High</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Daily incidents in context</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Incidents occur weekly</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Incidents occur Monthly or every few months</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Incidents occur at least once per year</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Very Low</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Incidents occur every few years</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Using the Probability and Impact descriptions choose a number that reflects the overall risk level for each threat.

Notes:

- Remember that each threat may vary in level geographically. It may be necessary to evaluate the risk by locality rather than nationally. For instance a border area may be a Level 4 risk of armed conflict while provinces closer to the capital may be a Level 2. Depending on the scale of the emergency situation you may have one
overall risk rating for the area or several within the affected zone for each type of risk. Risks may also vary due to different levels of staff vulnerabilities. For example, sometimes national staff may be at less risk in a specific area than international staff or vice versa.

- Where possible use previously reported incidents on various types of threats to justify the risk rating level assigned \((frequency, target, consequences)\). However, in a new situation where previous humanitarian responses have not recently been undertaken it may be necessary to use data from comparisons to similar interventions combined with what current information is available from local sources.

### Step Three: Methodologies for Reducing or Mitigating Risks

1. **Overview**

   Once the threats that may affect a humanitarian response have been identified, and the risk from each evaluated and rated, it is important to recommend risk mitigation strategies to address these concerns. While no two situations are identical, there are normally actions that can be followed to reduce exposure to risk. This is the critical step in ensuring that before committing staff, resources and your organization’s reputation to a response that you have taken all reasonable steps to minimize the risk. This is an essential component of **Duty of Care**.

2. **Methodologies for Reducing Exposure to Risk**

   In general, reducing exposure to risk takes two forms:

   - **Reducing the probability of an incident** (prevention)
     
     And/or

   - **Reducing the impact if an incident does occur** (reaction)

   2.1 Therefore strategies to reduce risk should focus on prevention and reaction. By doing this you can lower the initial risk rating you assigned each threat identified and thereby improve your ability to deliver emergency response programmes. It is important to remember that the goal of security risk management is not to put up
barriers to delivering programming but to enable organizations to stay engaged despite the level of risk.

2.2 Some suggestions for reducing risk are identified in the chart below. It is important to think in terms of PREVENTION first and then REACTION. Ultimately the objective is to reduce the overall risk rating level by implementing your risk mitigation strategies. However, in an emergency assessment it will be difficult to evaluate how these generalized recommendations may impact on the threat environment. Should a humanitarian emergency response programme be authorized a more detailed risk mitigation process would need to be undertaken focused on the actual areas involved, the types of programmes undertaken and the risk environment in that specific area.

<table>
<thead>
<tr>
<th>Examples of Strategies to Reduce Probability</th>
<th>Examples of Strategies to Reduce Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure all activities are conducting according to your Code of Conduct</td>
<td>• Develop contingency plans for all likely types of incidents</td>
</tr>
<tr>
<td>• Utilize the UNDSS Saving Lives Together (SLT) initiative if available</td>
<td>• Ensure that you have hibernation, relocation and evacuation polices for your staff or organization and provide guidance and support for partners</td>
</tr>
<tr>
<td>• Actively participate in the local ACT or other NGO Forum on a regular basis to discuss and share security information (or form one if none exists)</td>
<td>• Ensure all staff have first aid training and suitable first aid kits in offices and vehicles</td>
</tr>
<tr>
<td>• If your organization and partners have a security plan adequate to the needs of the emergency ensure it is used. If not, one must be developed prior to activities commencing</td>
<td>• Ensure that there are redundant communications systems and do not rely solely on mobile phones</td>
</tr>
<tr>
<td>• Provide security training for any staff deployed and any local partner staff involved in the response</td>
<td>• Ensure the location of suitable medical facilities are identified and medical evacuation policies in place if necessary</td>
</tr>
<tr>
<td>• Build a high degree of trust and acceptance in the local community</td>
<td>• Identify a crisis management structure to manage any incident to protect life, secure assets, secure the organization and protect programming</td>
</tr>
<tr>
<td>• Maintain an incident map to record where any incidents occur, what time of day, who was targeted, what actions were taken and the results of the incident. This helps staff planning work to avoid the highest risk environments.</td>
<td>• Have stress management and counselling services available including long term support in the event of a critical incident</td>
</tr>
<tr>
<td>• Investigate incidents and identify lessons learned. Share this information with other ACT members/NGOs</td>
<td></td>
</tr>
</tbody>
</table>

Example: Risk Assessment Report

The risk assessment report should include an overall summary that can be included in project proposals, event planning, travel plans and other types of activities. Should
reviewers require evidence of how you reached your conclusions, your can show your work with the more detailed threat reduction strategies as below.

### Risk Assessment Summary

Insert a short narrative of the overall risk assessment results

Example: Overall, the risk assessment for implementing this project is rated as 3: Moderate Risk. Staff will face challenges in building acceptance in the community and will be exposed to higher levels of risk for the initial stages of the program. Travel by road from the capital to project areas will be a primary risk as carjacking, robbery, and harassment at checkpoints is common. Staff will require security/first aid training and reliable communications equipment to implement this project. Teams should have contingency plans prepared for temporary hibernation or relocation from project areas if local security situation deteriorates. With proper security measures however, this project can be accomplished with a manageable risk level to staff.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Location</th>
<th>Initial Risk Rating</th>
<th>Reduce Probability Measures</th>
<th>Reduce Impact Measures</th>
<th>Risk Rating Lowered?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Vehicle Accident</td>
<td>All areas urban &amp; rural</td>
<td>3 High Risk</td>
<td>- Driver training</td>
<td>- Good first aid kits &amp; training</td>
<td>Yes, possibly to 3: Moderate risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Regular maintenance</td>
<td>- Medical insurance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Set speed limits</td>
<td>- Counselling for victims</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- No travel after dark</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. **Summary**

Risk assessment are key tools for almost all activities an NGO can undertake. It is a legal and moral responsibility for aid organizations in many respects. This includes:

- Program proposals
- Travel plans
- Conferences, workshops
- Emergency response
- All offices, compounds
- New security plans
- Where terrorism present
- Reputation risk concerns