Security Risk Assessment Tool

Version: (Draft) 24 April 2014

This tool was developed by the ACT Safety & Security Community of Practice (SSCP) for use by ACT Alliance members and partners.

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.

Step One: Identifying the Risks

1. Overview

There are many methodologies for identifying risks from actor mapping to complex context analysis. However, many of these require a significant amount of research and time in the region and may not be practical in an emergency assessment situation. However, if a response programme is undertaken these should be conducted within the first 10-15 days of deployment.

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?

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

List your risks:

Step Two: Evaluating and Rating the Risks

1. Overview

Once you have identified the types of risks you will face you will need to evaluate each risk and rate the level of risk. This is an important step to help the assessment team as well as their headquarters, their partners and any donors if applicable in understanding how you have developed your risk assessment.

The Threat	What Locations	Who/What will be at Risk?	What will the affect be?
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 govt* • *Reduction is ability to work*
Complete for each risk 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 this the following:

1. Very Low *2. Low* *3. Medium* *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.

Impact / Probability	NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
	No serious injuries. Minimal loss or damage to assets. No delays to programs.	Minor injuries. Some loss or damage to assets. Some delays to programs.	Non-life threatening injury. High stress. Loss or damage to assets. Some program delays and disruptions	Serious injury. Major destruction of assets. Severe disruption to programs	Death or severe injury. Complete Destruction or total loss of assets. Loss of programs and projects
Very Likely (Daily)	Low	Medium	High	Very High	Very High
Likely (Once per week)	Low	Medium	High	High	Very High
Moderately Likely (every year)	Very Low	Low	Medium	High	High
Unlikely (every 2 – 3 years)	Very Low	Low	Low	Medium	Medium
Very Unlikely (every 4+ years)	Very Low	Very Low	Very Low	Low	Low

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 threat rating for the area or several within the affected zone for each type of risk. Threats 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.

- 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 risks and threats that may affect a humanitarian response have been identified, 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 organizations' 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.

Examples of Strategies to Reduce Probability	Examples of Strategies to Reduce Impact
• Ensure all activities are conducting according to your Code of Conduct • Utilize the UNDSS Saving Lives Together (SLT) initiative if available • Actively participate in the local ACT Forum on a regular basis to discuss and share security information (or form one if none exists) • Actively participate in any other NGO security group, formal or informal, that meets to discuss the security situation in the country • 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 • Provide security training for any staff deployed and any local partner staff involved in the response • Build a high degree of trust and acceptance in the local community • 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. • Re-assess each threat and its rating in an ongoing schedule and adapt prevention strategies as needed	• Develop contingency plans for all likely types of incidents • Ensure that you have hibernation, relocation and evacuation polices for your staff or organization and provide guidance and support for partners • Ensure all staff have first aid training and suitable first aid kits in offices and vehicles • Ensure that there are redundant communications systems and do not rely solely on mobile phones • Ensure the location of suitable medical facilities are identified and medical evacuation policies in place if necessary • Identify a crisis management structure to manage any incident to protect life, secure assets, secure the organization and protect programming • Have stress management and counselling services available including long term support in the event of a critical incident • Investigate incidents and identify lessons learned. Share this information with other ACT members/NGOs • Have a good internal and external communications systems to control rumours and ensure the reputation of the organization is protected.