THE ASSESSMENT PROCESS

Assessing the security environment, identifying a potential threat, and reacting accordingly, is something everyone does every day, most of the time without notice. A staff member may choose a time and route to drive to minimize chances of an accident, or check the door locks each night to reduce opportunities for theft. The Country Office can use the same process to assess the potential for safety and security incidents and design appropriate and effective security measures. In many cases the process is routine, such as buying bottled water when the local source is thought to be contaminated. In other situations, such as in areas of instability or those prone to natural disasters, the assessment process can be more complicated.

A Safety and Security Assessment addresses factors that can contribute to the likelihood of a safety or security incident, including:

- Disregard for appropriate safety guidelines, such as for fire, medical and transportation.
- A rise in crime and banditry with the spread of small arms, a breakdown of law and order, and limited economic opportunities.
- The perception of humanitarian organizations as “wealthy” and “soft” targets.
- Increased exposure to violence as more agencies work closer to the center of conflict.
- The loss of perception of aid agencies and their staff as neutral, impartial and apolitical.
- The conscious manipulation of humanitarian needs and the presence and resources of humanitarian agencies as part of political and military strategies.
- The incorporation of humanitarian goods in the infrastructure of violent groups.

This chapter outlines the parts of the assessment process:

Safety and Security Assessment Procedures

Establishment of Country or Area Risk Ratings

Country Office Security Strategies

2.1 SAFETY AND SECURITY ASSESSMENT PROCEDURES

CARE staff at all levels should continually monitor significant political, social, economic, and military events in the areas where CARE works. But often those best able to conduct assessments in a specific country or region are the staff members working within them. Therefore, the Country Office (CO) has the primary responsibility for conducting the safety and security assessment and implementing measures to reduce vulnerability. A comprehensive safety and security assessment includes:

- An analysis of threats to CARE staff working in the area
- Identification of vulnerability to the threats
- Development of indicators and thresholds for threats to monitor change in the security environment
- Establishment of overall risk levels for the country or area

The assessment is not, however, a one-time event. It is a continuous process of collecting, analyzing, and using safety and security information. Situations in the field can change, sometimes rapidly and without warning. With each change, the risk to staff may increase or decrease, and security measures should be adjusted accordingly.

Prior to implementing any program, the CO staff — in coordination with the RMU — should carefully research the area to determine possible threats to staff and operations. There are a wide variety of political, economic, cultural and social issues to investigate, including:

- Geographical and environmental characteristics of the area, including the likelihood of disease and availability of treatment.
- Political and economic situation.
- Traditions, beliefs, customs and religious dynamics.
- The identity and ethnicity of the various groups in the area, especially during complex crisis.
- Identity and strength of authorities and development of local and national infrastructure.
- Attitude of the various groups toward CARE, other agencies and programs, and foreigners.
- The nature of the disaster, conflict or complex crisis during emergency response.

THREAT ANALYSIS

A threat is the possibility that someone or something can injure staff or steal or damage organizational assets. Conducting a comprehensive safety and security assessment includes an analysis of the threats the humanitarian organization might face and its vulnerability to them. Understanding the nature of threats facing the staff can help determine which security measures are most likely to ensure safety. The threat analysis process involves answering four key questions.

Who might wish to harm the organization? Possibilities may include dissatisfied workers, fired staff, guerrillas, bandits, terrorists, national and/or dissident soldiers.

What types of threats are present? Usually one of three main types.

> ***Crime*** *– performed through malicious, financial or personal motivation.*
>
> ***Direct threats*** *– where a specific organization is the intended target. The reasons for targeting may be political, economic, or military.*
>
> ***Indirect threats*** *– where an organization is not the intended target, but is unintentionally affected. Situations may include landmines, having staff members "caught in the crossfire" between belligerents, fire, disease, or a natural disaster.*

Why *might humanitarian workers be targeted? Reasons may be political association, robbery, retaliation, riots, ransom, rebel fighting, or threats everyone faces, such as indiscriminate shelling.*

How *might an incident take place? Are fires or natural disasters common? In areas with instability or high crime rates, are perpetrators usually armed? Are food and water supplies contaminated?*

Tools such as checklists, interviews or incident report forms can help answer these questions accurately. Sharing security information between NGOs or acquiring security information from national staff and contacts at friendly embassies also can provide reliable answers.

IDENTIFYING VULNERABILITIES

Vulnerabilities are situations or actions that can result in an organization having a greater chance of becoming a victim of a security incident. It is the level of exposure to a given threat. For example, a carefully shaped security profile and other measures may reduce the organization's vulnerability to theft even if the threat level in the area is considered high.

■ CHAPTER 2 THE ASSESSMENT PROCESS

Careful analysis of vulnerabilities can help in planning emergency actions and determining the required supplies and equipment. The same tools used to analyze threat levels can be used to identify vulnerabilities. Issues to consider when analyzing an office's vulnerabilities are:

***Where** are weaknesses that may increase the likelihood of an attack? This can include physical locations, such as residences, guesthouses, roadways, warehouses, offices, and remote sites. Or they may be operations, such as program, logistics, and finance activities.*

***When** is the humanitarian organization most vulnerable to attacks? Vulnerability may increase during transport activities, relief distribution, pay periods, and periods of civil strife.*

DEVELOPING INDICATORS

Certain events may indicate changes in the safety or security environment, which could then suggest possible modifications in safety and security procedures. These indicators vary from area to area and are identified during the assessment process. The box below mentions common indicators for an area of instability, but different indicators can be made for detecting disease epidemics, enhancement or degradation of medical treatment capabilities, crime, etc. All staff should be made aware of the indicators. Then, observation during the daily routine is usually sufficient to detect any changes.

THREAT INDICATORS

Military Preparations	**Local Expectation of Confrontation**	**Anti-NGO Sentiment**
Building/repair of military positions	Departure of families from area	Cold or harsh stares, hostile gestures directed at vehicles or staff
Military convoys on the road	Gathering of important possessions	Anti-NGO graffiti
Stockpiling of food and supplies	Extra buying/stockpiling of food and supplies	Light harassment of aid workers
Increased recruiting	Children staying close to home and parents	Open anger against NGOs
Departure of soldiers' families	Markets closed or hours reduced	Pilferage and theft by staff
Staffing checkpoints	People staying home at night	Vendors not selling to NGOs
Laying mines near military positions	People staying off the roads	Staff receiving threats

SECURITY THRESHOLDS

To complete the security assessment all Country Offices should identify security thresholds for their area. A security threshold, usually closely linked to threat indicators, is a readily identifiable "trigger" event that, when it occurs, automatically brings about changes in the office's security measures. For example, belligerents threatening the only airport in an area of instability may prompt the early evacuation of non-essential personnel and family members before air service is suspended. These thresholds must be defined for each area, since what is threatening for one region might not be as serious for another.

In the event of a crisis, making an objective decision about increasing security levels and when to evacuate can be difficult. With predetermined indicators and security thresholds, a Country Office can act quickly and appropriately before staff safety is threatened.

CONTINUAL SECURITY ANALYSIS

Threats and organizational vulnerabilities can change frequently. Therefore, continuous analysis of the environment is critical. Two methods, when used together, facilitate an ongoing security analysis:

- *Using the Who, What, How, Why, Where, and When questions detailed earlier*

- *Pattern analysis involves recording security incidents affecting CARE staff or involving another organization and identifying trends to determine possible changes in vulnerabilities. An incident viewed in isolation may indicate little, but when grouped with others may indicate a significant trend. This can aid in accurately predicting how situations and vulnerabilities might change, or determining appropriate modifications in the Country Office's safety and security procedures.*

2.2 COUNTRY RISK RATINGS

The completed assessment allows the National Headquarters, in coordination with the RMU and Country Office, to determine the level of risk present in a given area or country. Risk ratings are not based solely on the presence of threats. The likelihood and speed of changes in threats, the vulnerability of the staff to a specific threat, and the effectiveness of any safety and security measures already in place, are also considered when setting a risk rating. For example, there may be a significant threat of disease from contaminated water in a given area, but if the staff drinks and cooks only with bottled or filtered water, the risk of disease would be considered low. There are four levels of risk: Low, Moderate, High, and Severe.

Based on communications with the RMU and CO, the National Headquarters will review the risk rating of each country on a regular basis and revise it as necessary. Individual regions within a country may be assigned different risk ratings. High risk levels are generally associated with civil unrest and crime, but may reflect increased threats from disease epidemics or natural disasters.

LOW RISK

These are countries, regions, or cities that are essentially stable and free of political, economic, and social unrest. The crime is generally low and organized anti-government or terrorist groups, if present, exhibit limited operational capabilities. It is important to remember those countries with low crime and stable social systems may still have threats from natural disasters, such as volcanoes or floods. Normal security precautions are required in low-risk countries.

MODERATE RISK

These are countries or regions where low-level political, economic, and social unrest is present and/or where safety and security infrastructure (police or medical care for example) is poorly developed. Organized anti-government or terrorist groups may be active but not strong enough to threaten government stability. The country may be involved in a regional dispute, exhibit high crime rates, or prone to natural disasters or disease epidemics. Increased safety and security precautions are required in moderate-risk countries.

HIGH RISK

These are those countries or regions where organized anti-government or terrorist groups are very active and pose a serious threat to the country's political or economic stability. A civil war may be in progress and paramilitary or guerrilla forces may be in control of a significant area. Such a country might also be near or in the process of a military coup, be involved in violent regional disputes with its neighbors, or exhibit a breakdown in social infrastructure, especially police and judiciary. There may be prejudicial treatment of foreigners, or threats or harassment of NGOs or CARE specifically. Stringent security precautions are required in high-risk countries.

SEVERE RISK

These are countries or regions where the level of violence presents a direct threat to the safety and well-being of humanitarian aid workers. Operations are usually not possible without military support and security cannot be reasonably assured. There may be temporary suspension of operations, relocation of international staff, and/or additional precautions for national staff.

2.3 SECURITY STRATEGIES

An aid or relief organization working in an area where the greatest threats are from crime, instability, civil strife or conflict must have a clear and comprehensive strategy that addresses the risk to staff. A security strategy is based on the perception of the community where the agency works and the organization’s stated working philosophy. Some organizations rely on the goodwill of the local population for safety (Acceptance strategy). In other circumstances, humanitarian staff may require armed guards (Protection strategy) or even military units (Deterrent strategy) to provide a safe working environment. The choice of security strategy depends on the range of safety and security measures available. CARE Country Offices should continually monitor their working environment and their perceived position in it. Keeping a low profile or assuming protection based on “doing good work” is not a security strategy. An organization’s security strategy must be well thought out, carefully crafted and assiduously maintained in order to be effective. Generally, there are three types of security strategies a humanitarian organization may adopt:

Acceptance. Most aid organizations prefer an Acceptance strategy. It involves reducing or removing the threat by gaining widespread understanding and acceptance for the organization’s presence and work. The way a program is designed and carried out, and how the humanitarian organization reacts to events, must be transparent and consistent with the guiding principles it has been communicating. If a community or government clearly understands the organization’s purpose, it can become part of the security network, providing warning of possible changes in the security environment or mitigating their effects.

Protection. A Protection strategy usually involves implementing increased security measures, such as strengthening locks and barring windows, setting curfew or hiring guards for warehouses and offices. These efforts reduce the risk, but not the threat, by making staff and assets less vulnerable. Adopting a protection strategy almost always will require additional budgetary resources. The Country Office should ensure that the staff receives training on equipment and procedures. It also will need to be more attentive to stress management, since this strategy may impose restrictions on normal activities and freedom of movement.

Deterrence. Deterrence involves reducing the risk from instability or crime by containing and deterring the threat with a counter-threat. These may consist of supporting military actions, legal, economic or political sanctions or withdrawing agency support and staff. Single NGOs, including CARE, rarely possess a deterrence capability. However, during modern conflict, other organizations, such as the military (host nation, NATO or the U.S.) or UN troops may deploy their forces to support humanitarian aid and relief efforts. When considering deterrence as a primary strategy, the Country Office must have a clear understanding of the perception surrounding humanitarian actions conducted in conjunction with armed force. Staff should receive clear guidance on CARE International's policy on appropriate relations with military units and the appropriate use of armed protection.

CHOOSING A SECURITY STRATEGY

Many agencies have an institutional preference for one strategy or the other. After conducting a thorough safety and security assessment, and in coordination with the RMU and National Headquarters, the Country Office should choose the optimum mix of strategies for any given situation and be prepared to alter the strategy as the situation dictates.

These strategies are not exclusive. In practice, an agency may employ a mix of these or emphasize one more than another in different operational areas of a country. The attempt to gain acceptance and consent may be combined with protective measures where crime and banditry remain a real threat that the authorities and the population themselves do not have the ability to control. Use of deterrence, usually in a military context, may facilitate delivery of aid in conflict settings, but protective measures for CARE assets may still be required.