Security Management

Modifying CARE International Operations due to Security Conditions

TABLE OF CONTENTS

MODIFYING CARE INTERNATIONAL OPERATIONS DUE TO SECURITY CONDITIONS

The guiding principle for all CARE International (CI) security policies, programming, and the CARE International Safety and Security Unit (CISSU) is that the **"safety and security of CARE staff always take precedence over all other factors."** This standard serves as the foundation for the common understanding of staff welfare, defining security actions, and actively involving CARE staff in safety and security initiatives. With this foundation, organizational decisions regarding presence issues have to be taken anew in each situation.

Balancing a threat to staff with the humanitarian imperative. In defining levels of presence and engagement, a tendency exists to look for definitive criteria that will generate an automatic response. While we can define the threats with a degree of certainty, the humanitarian requirement, training, and awareness of CARE staff; presence of well trained armed forces such as NATO or military personnel associated with the United Nations; and other factors mitigate a number of the threats and vulnerabilities. Consequently, the CISSU has designed criteria that require a dialogue within line management to examine conditions and to set accountability when security becomes a consideration in a country office or presence.

In preparing this paper, a number of senior managers throughout CI asked the CISSU to "build a set of triggers which will evoke a closure of a country office or lead member presence." We began this initiative with that focus. However, it soon became apparent that every situation is context specific.

Background

In response to the request to formalize a mechanism to examine presence issues, the CISSU designed a set of criteria, which, when adopted by CARE International as policy, will serve as the basis for examining conditions and determining whether or not to modify operations. In building these measures, we focused on the fundamentals of risk. From a security standpoint, risk is associated with conditions that increase the likelihood of harm or loss occurring to CARE staff members, property, or the organization's operations. Clearly defining CARE International's risk tolerance is a critical first step in making good decisions about modifying operations. What is the amount of risk CARE is willing to accept and what costs and losses can be tolerated that are associated with the risk? Quite literally, what is the potential cost of doing business? This applies to people, property, and organizational reputation.

**Risk:
The possibility
of suffering
harm or loss**

This is a difficult topic to address. However, to make the best decisions on whether to modify operations, risk-tolerance levels and acceptable costs must be established.

Note: A single level of risk tolerance cannot be uniformly applied to all CARE operations. For example a higher level of risk may be acceptable in a food distribution operation that directly saves lives in the short term, compared to a micro-finance program that, while important, doesn't have the same immediate life-saving characteristics.

Defining Risk Levels

To make effective decisions on whether to modify operations because of security conditions, we must define our risk levels. The inability to articulate "conditions" elevates risk because the probability of harm or loss may go unrecognized. Considering this, CISSU established a baseline that defines security conditions. Throughout CARE International, we define risk by four categories, as shown in the table below.

Categories of Risk
LOW: Normal security precautions
• Countries, regions, or cities that are essentially stable and free of political, economic and social unrest. • Crime is generally low and organized anti-government or terrorist groups, if present, exhibit limited operational capabilities. • Threats of natural disasters and disease still exist.
MODERATE: Increased safety and security precautions
• Countries or regions where low-level political, economic, and social unrest is present and/or where safety and security infrastructure 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 epidemic.
HIGH: Stringent security precautions
• 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 a paramilitary or guerrilla forces may be in control of a significant area. • May be near or in the process of a military coup, be involved in violent disputes with its neighbours, or exhibit a breakdown in social infrastructure, especially police and judiciary. • There may be prejudicial treatment of foreigners or specific threats to NGOs and/or CARE. • Civil unrest and crime are present but these may also reflect increased threats from disease epidemics or natural disaster.
SEVERE: Temporary suspension of operations, relocation of international staff, and/or additional precautions for national staff
• Levels of violence present 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 operation, evacuation of international staff, and/or additional precautions for national staff.

Criteria to Elevate or Lower a Threat Level

The Designated Member or Regional Director is responsible for monitoring the situations in all Country Offices (COs) or temporary presence activities and recommending a change of risk level (up or down). This should be done quarterly or as needed when significant activity is occurring in the country (elections, demonstrations, abnormal actions by government authorities, etc.). The CO can also recommend to line management that a risk level be raised or lowered according to the changing situation.

Upon observation of any of the above change-of-risk-level thresholds, a security assessment of the situation should be conducted. In addition, indicators must be monitored for signs that a change of risk-level in a downward direction can be implemented.

Criteria to Elevate a Threat Level

LOW to MODERATE

- The country starts to see a slow or rapid increase in political, economic, or social unrest
- Obvious increase in personal and property crime or governmental reports of significant increases in crime

MODERATE: Increased safety and security precautions

- Anti-government or terrorist groups have begun to emerge and have threatened the government or infrastructure
- Outbreak of conflict, internal or external, between two or more actors to include criminal, clan, insurgent or national or paramilitary elements
- Deterioration of governmental control within its borders
- Possibility of coup d'etat
- CARE must limit/prohibit travel occasionally until the situation becomes secure (once a month or more)
- Verified targeted harassment and threats against foreigners, members of international organizations or any CARE staff by known or unknown entities
- Increased security measures (physical and/or policy) needed in order to operate safely

HIGH: Stringent security precautions

The potential for violence toward CARE staff is of such a nature that prudent measures for personal safety and security cannot be effectively employed. Therefore, CARE must consider suspension of operations for conditions such as:

- Areas in which CARE works see an increase in violence to the point that programming is frequently suspended (i.e., more than three times a month)
- Frequent relocations from program areas occur
- CARE must use armed escorts in order to move.

When do we consider closure, suspension, or modification of program delivery?

- When the true risk level is unclear, consideration must be given to temporary suspension of programming until a security assessment can be conducted (e.g., on rumors of fighting in a program area, programming may be halted until confirmation of the situation)

- Direct threats against CARE may necessitate temporary suspension of programming until a security assessment or negotiations can be conducted

- Risk to CARE partners (as a result of being involved in the CARE program) exceeds the benefits of the program. Risk of working for an international organization elevates the potential of life-threatening risks to CARE national staff and beneficiaries

- Continued operations may lead to due diligence/negligence/liability claims against CARE

- Security risk to CARE personnel temporarily outweighs the benefits of that program (e.g., there are life-threatening risks for CARE personnel in an area where programming does not include life-saving measures)

- Direct targeting of CARE programs/assets/personnel

- Direct targeting of the programs/assets/personnel of other agencies

- Secure operations in the environment are cost prohibitive (e.g., in high-risk areas an extensive communications network would be necessary for the security of staff, but funding is not available)

- Operating in the environment requires violation of humanitarian principles (e.g., in a conflict area where the government insists that aid can only go to a certain sector of the population)

- When it is deemed unacceptable to continue working in an area where the government or local authority is either unwilling or unable to provide NGOs with the same level of security/protection as is provided to citizens (e.g., the authority is unwilling to prosecute those accused of attacking NGOs)

- Phase IV evacuation indicators have been observed in the area of programming (see the evacuation plan portion of the Security Management Plan template)

- To be used as a tool for advocacy (with careful consideration—CARE must maintain its primary responsibility to those in need)

- Continued operations may pose enough potential damage to CARE's reputation that it may affect CARE operations worldwide

- National government or other powerful actor demands/requests our immediate departure

When do we commence evacuation measures?

Circumstances that might require evacuation of staff and/or their families to a site outside the country or area include mounting terrorist activities and threats, insurrection and other civil disorder, or a sudden crisis such as a natural disaster. Evacuation should be considered as a last resort after efforts to resolve or mitigate potential threats are unsuccessful.

In most cases, the designated member, in consultation with the Country Director, CISSU, CEG and RMU, will make the final decision to evacuate. In the event time or communication difficulties make coordination impossible, the Country Director or temporary presence coordinator has the authority to order and conduct an evacuation.

Criteria for evacuation

There are a variety of indicators for evacuation, including:

- Are staff members exposed to increasing and unreasonable risk?
- Have other agencies (UN, Red Cross, etc.) or the government recommended departure? What actions are other international NGOs taking?
- Have the embassies advised foreign nationals to leave?
- In lieu of evacuation, what measures can be taken to ensure staff safety, such as curtailing operations or relocation in-country?
- What is the impact on the safety of national staff if international staff depart?
- Is there a requirement to evacuate or relocate national staff members and their immediate family?
- What is the possibility of meeting current project objectives safely?

When do we evacuate non-essentials

In any designated high-risk country, the presence of dependents and/or non-essential staff will be evaluated and justified by the Designated Member. For example, if the country is designated as high risk, but dependents are located in a moderate-risk location, consideration may be given for their continued presence. However, the norm for a high-risk environment is the exclusion of dependents.

When do we review the status for accompanied or unaccompanied posts

- When the country has been rated as high risk and there is no potential for improvement in the foreseeable future
- When the status quo includes the presence of at least three Phase III evacuation indicators:
  - 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 a paramilitary or guerrilla forces may be in control of a significant area.

– May be near or in the process of a military coup, involved in violent disputes with its neighbours, or exhibit a breakdown in social infrastructure.

– There may be prejudicial treatment of foreigners or specific threats to NGOs and/or CARE.

– Civil unrest and crime are present, but there may also be increased threats from disease epidemics or natural disaster.

Planned Responses

A planned and structured response in deciding whether to modify operations is the most effective and efficient approach to handling potential change. A standardized decision-making process that uses both objective and subjective information eliminates many of the problems associated with unplanned reactions to crisis events.

Planned responses rely on trigger events. A trigger event is a set of conditions or incident(s) that, when present, prompts discussion and decisions, in this case whether or not to modify operations. Three types of trigger events—abnormal conditions, crisis events, and predicted events—can be used in making modification-related decisions: These types of trigger events could be used individually or together as part of a decision-making system.

Trigger Events

- Abnormal conditions
- Crisis events
- Predicted events

Abnormal conditions

Once baselines for security conditions and operational status have been established, normal conditions can be compared against current conditions to determine if a modification is warranted. For a security conditions baseline, the ratings associated with various factors (terrorism, criminal activity, political instability) can be quantitatively examined to determine the variation from normal. If certain thresholds are reached or there is a significant amount change, these may be trigger events for modifying operations.

For an operational status baseline, if security conditions cause the office capacity to fall below a certain level for a sustained period, it is prudent to have a discussion about modifying presence or operations.

When using abnormal conditions as trigger events, in addition to knowing the amount of change from normal, it is also important to consider five other factors, as shown below. Asking these questions helps to put the abnormal conditions in better context so informed decisions can be made regarding the level or status of operations. In addition, these five factors can be used to form very specific decision-making criteria. The table below suggests theoretical examples for suspending operations using operational status as a trigger event.

Context for Abnormal Conditions		
Factor	**Definition**	**Theoretical Decision-making Criteria**
Impact	The impact the abnormal conditions currently have on CARE operations (or other humanitarian organizations)	Normal operations are at 50 percent or less of capacity
Duration	How long abnormal conditions have been occurring	Abnormal conditions have been ongoing for a period of three continuous weeks
Location	The distance away from the operating area where the abnormal conditions are present	Abnormal conditions exist within a 50-mile radius of the operations area
Trend	Whether abnormal conditions have been improving, degrading or are unchanged	Conditions are degrading or unchanged
Response	The actions CARE has taken to respond to abnormal conditions (whether risk is being effectively mitigated)	Appropriate security measures have been applied based on the threat(s) but are unable to raise operations above a 50-percent capacity level

Crisis events

Crisis events are predetermined security events or conditions that immediately trigger discussions and decisions on whether to modify operations. An example would be the violent death of a staff member or a World Health Organization Phase VI pandemic alert. Using agreed-upon crisis events as triggers for suspension discussions and decisions (with linked response plans) is a simpler approach than using the abnormal conditions method since not as much monitoring is required.

Predictive events

Predictive modeling involves using quantitative data to forecast an outcome. Based on previously collected data from situations involving program or presence modifications, trends and patterns may emerge that predict the likelihood of modification. Predictive events can serve as an early warning system for reducing the chances of a crisis event occurring.

At the present, there is an inadequate amount of quantitative data to use predictive modeling as a decision-making tool for suspensions. However, as the CARE Security Incident Monitoring System (SIMS) is deployed to the field and a sufficient amount of analysis data becomes available, predictive modeling data should be incorporated as part of the decision-making process.

Mirroring Other Organizations

Mirroring other humanitarian organizations' decisions on modifying operations because of security conditions is common. However, this can produce a cascading effect, with other organizations quickly following modification, suspension, or withdrawal. Alternatively, donor pressure, public relations issues, or institutional culture may compel an organization to continue operations while others have withdrawn.

Because unilateral modifications can jeopardize relationships with other humanitarian organizations, CARE should consider entering into cooperative agreements with other organizations in the area of operation for collective security engagement. All cooperating organizations would be using the same objective criteria for security-related decisions.

If a joint decision strategy is pursued, all of the cooperating organizations need to have similar levels of risk tolerance. Too much variation in risk tolerance means that organizations will not be able to come to a consensus agreement on suspension. Organizations should be compared with CARE at the field level and classified accordingly (see box).

Classification of Risk Tolerance Compared to CI

- Significantly More Risk Tolerant
- More Risk Tolerant
- Slightly More Risk Tolerant
- Same Risk Tolerant Level
- Slightly Less Risk Tolerant
- Less Risk Tolerant
- Significantly Less Risk Tolerant

Conclusion

In today's world, CARE faces the challenge of balancing threats to staff with its humanitarian imperative and has thus charged the CISSU with formalizing a mechanism to examine presence issues. The original focus on creating definitive criteria from which to generate an automatic response was quickly eclipsed by the fact that context-specific factors can mitigate a number of threats and vulnerabilities.

Focused on the fundamentals of risk, CISSU has designed baseline criteria against which line management can conduct a dialogue, examine conditions, and determine accountability. These criteria address how to establish risk-tolerance levels and acceptable costs so as to make the best decisions on whether and how to modify operations when security becomes a consideration in a country office or presence.