CARE International
Critical Incident Policy

Introduction

Critical incidents, including kidnapping, abduction and hostage taking are an increasing threat to humanitarian workers all over the world. For this reason it is imperative that all CARE International members prepare for worst case scenarios and harmonise principles and policies to prevent incidents from occurring and, if they do, manage them successfully. Anticipating and preparing responses will facilitate a more positive and timely recovery during critical incidents, reducing the impact on staff and the organisation. This policy describes CARE International's prevention and preparedness for a critical incident and its response should one occur.

A Critical incident is defined as an incident that: significantly disrupts an organisation's capacity to operate; typically life is lost or threatened, or the incident involves mortal danger[1].

A critical incident could be, but is not limited to, any of the following:

- Abduction
- Arrest
- Assault
- Death of a staff
- Detention
- Hostage taking
- Kidnapping
- Missing staff
- Natural disaster
- Public violence
- Sexual assault

[1] Good Practice Review 8: Overseas Development Institute (UK: Humanitarian Practice Network, 2010)

Principles

Each member of CARE International (CI) will endeavour to have specific prevention and risk mitigation measures to promote the safeguarding of personnel from critical incidents. This includes the adherence and reinforcement of the guidance stated in the CI Personal Safety and Security Handbook and the CI Safety and Security Manual. Prevention and risk mitigation measures include the discretion of relevant Human Resource staff to identify at risk personnel and to discourage their deployment to or else modify their level of exposure.

All CARE International Members shall have situation-specific and global preventive measures including minimum training standards, pre-deployment and in-country briefing requirements, development and communication of context/country specific standard operating procedures (SOP's) and policies that reflect proper and updated situation and risk analysis.

In addition, CARE International Employing Members (EM's) are the default final decision making authority in any critical incidents involving their staff.

Country Offices (CO's) are accountable for contextual and risk analysis as well as risk reduction through essential training, SOP's and policy. Most importantly, CO's will ensure compliance of global and situation-specific policies and procedures to foster individual awareness and preparation. CO's will ensure accountability and will base good programming on striving for positive community acceptance, which in itself is both an effective deterrent mechanism and tool during critical incident management. It is the responsibility of the LM to ensure the CO has adequate support to meet their responsibilities[2].

CARE International Safety and Security Unit (CISSU) has the responsibility to harmonise responsibility and good practice by developing and establishing accepted principles and policies in order to implement organisation-wide standardisation and implementation of preventive and management strategies.

Individual staff members are required to maintain awareness of who they are, where they are, how to reduce their exposure (input into and compliance with SOP's and policies, good personal habits) and know how to react/survive in critical incidents. Staff must also be aware not to increase risks to other personnel (local staff and communities) by their actions.

[2] CARE International Code, Section 12, CI Safety and Security Principles, Principle 5, Standard 1

Preparation

Safety and Security Policy, Procedure and Contingency Planning. All CO's will have a safety and security plan that encompasses both preventive and reactive measures for critical incidents. These plans will consider the CO's context specific risk and propose adequate mitigation strategies. Contingency plans will be written and distributed to relevant staff, or groups of staff, according to their roles and responsibilities in critical incident management.

Training. Relevant staff[3] will receive training according to the context-specific level of risk for critical incidents. Critical Incident Management teams must undergo training to promote understanding and rehearsal of their roles and responsibilities. These trainings may vary from scenario based exercises to formal workshops at either local or regional level.

Insurance Coverage. Insurance coverage is a crucial issue. All CI staff must be adequately insured for the country(s) of destination. The insurance should cover illness, accidents, medical evacuation, and repatriation. Special care must be taken that insurance coverage is adequate for the level and nature of risk (e.g. conflict zones, where relevant) and that staff are aware of any exclusions[4].

1. Underwriters. The insurance policy underwriters must be fully aware and familiar with CARE International's operational profile and areas of work. Underwriters of the insurance policy will factor in conditions for the activation of, or access to, provided third parties.

2. Activation of third Parties. As part of a coordinated response to a critical incident, the relevant CI stakeholders will coordinate the activation of third parties.

3. Resources. The management of critical incidents requires robust financial resources and management systems. Contingency funds must be available and budgeting for contingency funds is required of all CI members.

   Expertise and human resources across CI shall be made available and shared.

[3] Relevant staff can refer to full-time, part-time and external staff such as consultants, interns, trainees etc depending on the specific situation

[4] CARE International Code, Section 12, Guidelines & Procedures for Safe Travel to Country Offices par II, 1, f

Roles and Responsibilities

Reporting and coordination of roles and responsibilities. Each critical incident is different and will thus be managed differently. However, the following coordination mechanism will ensure that roles and responsibilities are quickly and effectively allocated in order to ensure the incident is managed as well as possible.

1. CO's will immediately advise an EM, where relevant, if a critical incident occurs involving an EM's staff member.

2. The relevant LM will immediately advise the CI Secretariat when a critical incident occurs and the CI Secretariat, EM and LM shall immediate convene a meeting with all relevant CI stakeholders to determine specific roles and responsibilities. The CI stakeholders will include the CI member of the staff member's nationality, where necessary, as they will most likely be involved in family and media liaison. The EM will either be confirmed as the final decision making authority or the EM may decide to relinquish authority to the LM.

EM's may cede their final decision making authority to the LM should they decide the LM is better placed or as a result of a lack of skills, capacity and/or competency. This will be documented.

Employing member. The EM is the default final decision making authority in all critical incidents involving its staff.

Lead member. The relevant LM is responsible for the operational management of all critical incidents in CO's they manage.

CARE International Secretariat. The CI Secretariat is responsible for streamlining communication, ensuring coordination and resolving disputes between members during critical incidents.

Effective Critical Incident Management

Identifying management capacity requires the establishment of clear lines of authority and coordination as early as possible during a critical incident so a response can proceed quickly and without distraction from internal confusion and fracturing within the CI membership.

Operating principles

1. Decisions and actions are consistent with existing CARE policies and must not compromise operational management responsibilities on the ground.
2. Clear leadership and decision making lines.
3. Informed decision-making.
4. Need-to-know basis.
5. Communication Management.
6. Consistency with legal requirements including obtaining authority to act on behalf of a victim and whether we have the authority to disclosure personal information.

Development of a Strategy. Developing a strategy as early as possible during a critical incident is essential for an effective response.

Professional support. All CI members will have access to third parties e.g. private crisis management companies. Third parties exist solely to assist in the management of a critical incident. Professional support may also be required for psychosocial or other support.

Coordination.

1. Sharing of roles and responsibilities between CI members. The CI Secretariat, EM and LM shall immediate convene a meeting with all relevant CI stakeholders to determine specific roles and responsibilities. The CI stakeholders will include the CI member of the staff member's nationality if applicable.

2. Coordination with authorities. Coordination with national and host governments essential to effective critical incident management. The establishment of local and international security networks and liaising with an appropriate cross section of interlocutors must be considered and maintained.

   Working through local leaders and intermediaries requires a strong independent approach. Although it may not be effective in every case, it is a viable option that should be considered as part of an acceptance strategy.

3. Family Liaison. The family members of an affected staff must be consistently and continuously kept informed. The family liaison strategy and protocol must be established and considered at all levels of a crisis management plan. External, professional support could be considered as could the support of another CI member where relevant e.g. the member of the staff's nationality. Direct correspondence with family members should never be delegated to a field response team.

4. Communications[5]. There must be a strategy put in place that includes clear communication lines internally and externally with authorities, the media, family members, CI members, staff, donors and any other relevant stake holders. There should be one primary channel of information and authority from the Critical Incident Management Teams at CO, LM, EM and CI levels. The release of any information must be decided upon in coordination with management teams at all levels.

   The following are principles for good information management during a critical incident:

   - Accurate and Rapid. Critical information needs to be collected, verified and, where necessary, shared as quickly as possible.

   - Written. A lot of information will be transmitted orally but it is essential that important information, specifically information received and decisions made are documented and centralised.

   - Sharing. The Critical Incident Management Team at CI/Member level will determine what information is sensitive or not and how it is to be communicated and to whom. The basic principle of communication sharing is that each decision maker will have access to the information they require to make informed decisions. Sensitive information will be transmitted securely and only to those that need to know.

   - Sensitive information. Communication is critical during the management of a critical incident. Whilst there is a need to for communication to be clear and unambiguous there are associated risks as information is vulnerable to interception and distortion by people or groups for personal gain. For this reason the utmost care must be taken to ensure that documents do not contain information of a military/security nature or contain subjective and opinionated statement on controversial or political issues. Although some

[5] Further reference: CARE International Code: Section 11, Media and Communications

documents may require information of general military or political scenarios, the content should never be of a nature that would question CI's objectives and presence.

The unauthorised disclosure of sensitive information can be detrimental to CI's integrity and presence. Staff must be mindful of the misuse of sensitive information and its impact on the safety and security of its staff and assets. Each LM member shall have an approved information disclosure policy entailing rules and regulations governing the collection, storage, and dissemination or information[6].

Access to safety and security or other sensitive documents shall be restricted to an identified number of persons and granted on a strict need-to know basis.

Document and data storage will undergo routine backing up. The storage of sensitive data will be protected where necessary.

- Internal Communications. Internal communications need to be managed at different levels. Some information will be classified as confidential or internal and the dissemination of such requires discipline. Sharing updates demonstrates a certain level of transparency while alleviating speculative and rumour based ideas or statements.

  Personnel of the affected CO may feel a desire to be directly involved and informed. Depending on the circumstances daily briefings during the first stages of the critical incident are advised until regular updates are given as the situation continues.

  Those responsible for dealing with families, other LM's, authorities, media, donors etc. will require regular updates or situation reports.

  Other CO's and LM's need to receive updates due to geographical proximity or relationship to the affected CO.

5. Media Strategy and Coordination. Strong CI media coordination is essential during critical incident management. The response team approved media strategy overrides individual members' media interests and must be given high priority. This includes establishing and rehearsing a media strategy plan.

   Specific attention must be paid to the use of social media by staff, family members or other. Mechanisms to monitor social media must be put in place in order to limit any possible damage.

[6] Further reference: CARE International Code: Section 11, Media and Communications

6. Legal Aspects. CI members must consider all legal implications of a critical incident. Legal action can include allegations of negligence, neglect or unreasonable action. Documentation of the incident and all relevant information is essential in such cases.

After action Reviews

Analysis of the incident and proper transference of lessons learned are good practice and should be completed as soon as possible after an incident. After action reviews must be shared and acted upon throughout CI.