



**CRITICAL INCIDENT MANAGEMENT  
IFRC CONTRY CLUSTER OFFICE  
FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY**

**Reference:** CRITICAL INCIDENT MANAGEMENT WITHIN FEDERATION  
OPERATIONS

Document authorization				
Stakeholder	Name	Position	Signature	Date approved
Author	Alexandre Claudon de Vernisy	Head of Country Cluster Office		
Document authorizer	Walter Cotte	Director, Americas Region		
Regional Document Stakeholders	Jorge Zequeira	Security Consultant / Coordinator		
Document stakeholders	Lars Tangen Jullian Harris Karl Julisson	Security Unit, Geneva		

**Definition of a Critical Incident**

A situation that, threatens, or has impacted on, the safety / security of Federation personnel, assets or operations to the extent that there is the potential to be a significant disruption or even incapacity to continue to operate.

The term **situation** is used in the definition so as to be sufficiently broad to encompass, specific situations e.g. death of a delegate or third party caused by Federation personnel, accidents with serious or multiple injuries, violation of status agreement, kidnapping; or a major disruptive events such as a building fire or pandemic.



**CRITICAL INCIDENT MANAGEMENT  
IFRC CONTRY CLUSTER OFFICE  
FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY**

	<b>Minor Critical Incident</b>	<b>Significant Critical Incident</b>	<b>Major Critical Incident</b>
<b>Description</b>	Incidents that cause minor disruption to the Federation's Regional operations e.g. vehicle accident without serious injury, theft, burglary. <sup>1</sup>	Incidents that cause significant disruption to Federation operations e.g. accidental death of a delegate, accident with serious or multiple injuries etc. <sup>1</sup>	Incident that jeopardizes Federation's operations or that incapacitates the local office's ability to function. e.g. serious deterioration in security situation, multiple loss of life, violation of status agreement, major equipment loss, office fire, pandemic etc. <sup>1</sup>
<b>Management Approach</b>	or senior manager <sup>2</sup> manage the incident, and <b>Head of Country Cluster</b> .  <b>Zone Security Coordinator and Director of Zone</b> advised through incident reporting procedures.	Security Coordinator and <b>Head of Country Cluster</b> manage incident with advice and if required direction provided by Director of Region and Geneva SMT	Incident managed through Geneva, field teams provide information and act on direction from the critical incident manager, a support team may be deployed in the case of a field incident.
<b>Reporting Requirements</b>	Normal incident report <sup>3</sup>	Immediate verbal report via telephone	Immediate verbal report via telephone

<sup>1</sup> The examples given are not exhaustive, but designed to be indicative.

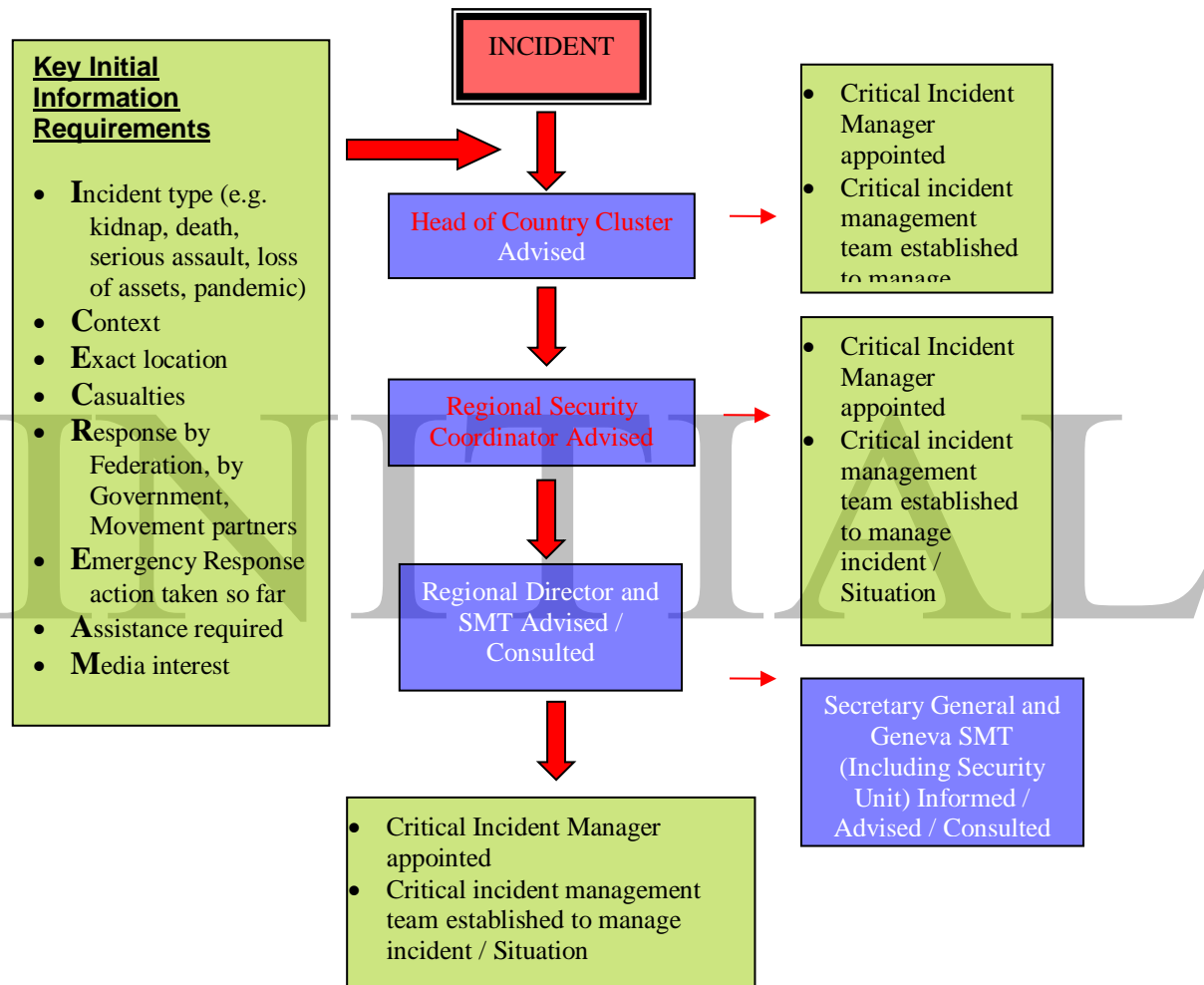
<sup>2</sup> The term Senior Manager is used as a generic term, dependent on the situation in the field this could be a Head of Operations or a FACT/ERU Team Leader.

<sup>3</sup> Security incident reporting procedures are outlined in the Security Section of the Fed Net - go on Fed Net-secretariat-security and then incident reporting.

**CRITICAL INCIDENT MANAGEMENT  
IFRC CONTRY CLUSTER OFFICE  
FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY**

**NOTIFICATION AND RESPONSE PROCEDURE**

The notification and response procedure for significant and major incidents is as follows:



**I. Immediate Response:**

The document below outlines the basic procedures to be followed in response to a critical incident within the IFRC COUNTRY CLUSTER OFFICE

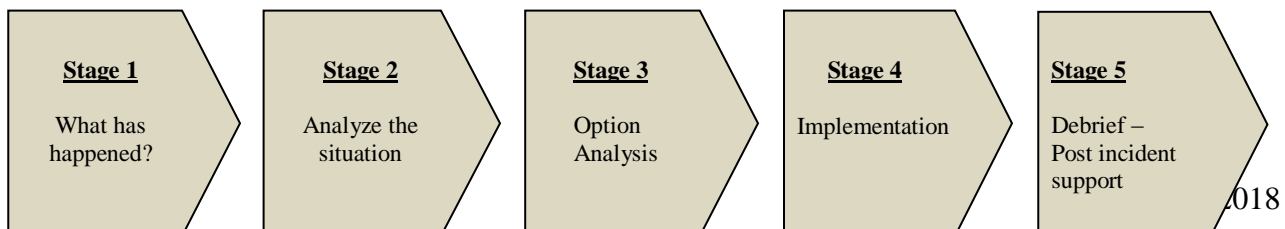


## CRITICAL INCIDENT MANAGEMENT IFRC CONTRY CLUSTER OFFICE FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY

- 1) Incident reported to **Head of Country Cluster Office**
- 2) **Head of Country Cluster Office** calls until one is reached, who then informs the others on this list:
  - **Security Coordinator Americas Regional Office (ARO)**
  - Director of IFRC Americas Regional office (ARO)
  - Security Unit in Geneva informed
  - **Argentina Red Cross Secretary General (or Country NS Secretary General, depending of he country where the incident occurs)**
- 3) **Head of Country Cluster Office** contacts local authorities in the area (police, 107, 911, **Argentina RC**, SINAPROC, fire brigade, etc.) and requests assistance.
- 4) **Head of Country Cluster Office** SMS Alert of incident to all staff to ensure no more staff members are exposed to the danger.
- 5) **Head of Country Cluster Office** commences collecting information on the incident to advice Security Coordinator and Director of Americas Region.
- 6) **Head of Country Cluster Office** and **Finance Senior Officer** inform Insurance Provider, GVA and family members (as applicable).
- 7) **Head of Country Cluster Office**, Director of Region and **Security Coordinator** form Critical Incident Management Team (CIMT – including staff members as outlined above), either chairing it himself/herself, or appointing a Critical Incident Manager (CIM), who directs resources as needed.
- 8) The CIMT takes over all line and operational responsibilities of the incident (as per the process outlined below), report directly to the Director of Region who retains overall authority.

### II. Critical Incident Management Process:

Usually includes five stages as per the diagram below:





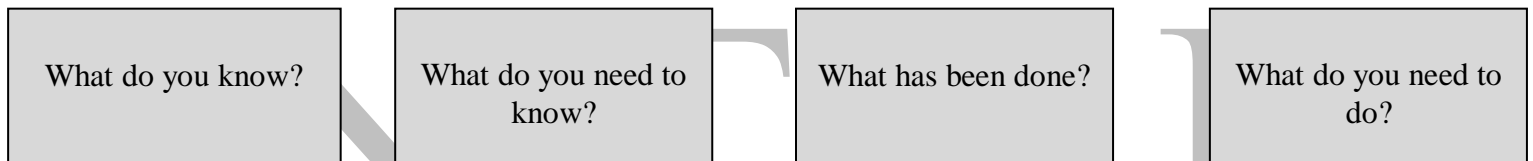
## CRITICAL INCIDENT MANAGEMENT IFRC CONTRY CLUSTER OFFICE FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY

### Stage 1: Establishing What has Happened

The first action must be to identify whether there *is any immediate action required to protect life, liberty, limb or eyesight – if so this must be taken.*

Verifiable information must be established outlining the details of the incident and an incident log is to be initiated. This is to record the chronology of events, log phone calls, record notes of all meetings and ensure all documents are recorded and filed.

### Stage 2: Analyse the situation / Map the playing field



The primary aim of this stage is to identify the problem and the parameters surrounding the problem:

- RC Movement actors involved (ICRC, IFRC) and current status (locations, operational agreements in force)
- Security issues
- External actors involved
- Country context – current situation (disaster, conflict etc.), infrastructure (transport, medical, food and water, sanitation), capability of Government, status and capability of NS in country, status of Federation in country, limitations on ability to act and operate.
- Legal issues
- Medical issues
- Communications issues
- Media issues
- Determine the end-state objective (injured person evacuated, body repatriated, hostage released)

The CIMT must also decide:



## **CRITICAL INCIDENT MANAGEMENT IFRC CONTRY CLUSTER OFFICE FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY**

- Whether due to risks to personnel, any programme activities should be suspended or whether personnel should be withdrawn to a more secure location.
- If additional support personnel should be deployed to any field location to assist.
- What information should be circulated internally and externally, and identify any limitations or confidentiality issues.
- If any additional personnel or external specialists should be included in the CIMT.

CIMT members may be assigned specific roles/tasks and responsibilities for managing relations with specific stakeholders.

### **Stage 3: Option Analysis**

At the start of this stage two questions must be asked:

- Is this situation covered by existing contingency plans – if so, can they be implemented?
- Is the situation severe enough to warrant the activation of a business continuity plan?
- Does the Federation have the internal expertise to manage the incident – if not, where can this be accessed?

If there are no existing contingency plans or no existing continuity plans that can be adapted, then a response plan must be developed. This requires the identification and analysis of options to reach the end-state objective(s). During this stage the following should be considered:

- Only options and factors that contribute to the identified end-state should be discussed and analysed.
- Options should have technical input from all members of the CIMT.
- If technical input is required that is not available from CIMT then it must be obtained.
- Options tested against:
  - Fundamental principles
  - Code of conduct
  - Limitations imposed by country context
  - Resources available to implement
- Preferred option is identified by members including the Security Coordinator, and presented for approval and action of the Americas Director of Region and country's RC Secretary General.

When considering options and having identified the preferred option the CIMT must always consider the fluid nature of the situation and the potential implication this might have – the



## **CRITICAL INCIDENT MANAGEMENT IFRC CONTRY CLUSTER OFFICE FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY**

question ‘**What if?**’ (something changes or something new happens) should constantly be tabled.

### **Stage 4: Implementation**

Implementation of the preferred option should be in the form of a plan. This should:

- Clearly define the objective(s)
- Assign clear roles
- Detail clear coordination aspects – timings, reporting requirements, interaction with other players – ICRC, Panamanian RC and/or external
- Define a clear command and control framework
- Information flow – the CIMT needs to ensure that Federation Media and External Communication Department, ICRC and Panamanian RC are kept informed on the need for control over information to the press/media and information sharing with our stakeholders. This might involve information black outs or preparing press lines, media statements and internal information sharing with the Panamanian RC.

The CIMT’s role is to monitor the implementation and be prepared to adjust actions and plans as required.

### **Stage 5: Follow Up/Debrief**

After the incident has been resolved a debriefing process is to be implemented. In the first instance, the incident and situation surrounding the incident is to be fully investigated to determine why it occurred, whether it could have been prevented and how to prevent it in the future. Secondly, the debrief is to examine how the incident or situation was managed, in order to determine what can be learned and whether the manner in which it was managed could be improved. This process is to work through the incident chronologically (from start to finish) and examine actions taken at each stage.

- Confirm the incident log and sequence of events is accurate
- Were the actions taken appropriate?
- Were the existing procedures followed and are these procedures appropriate or do they need changing?
- Lessons should be identified and recorded
- Are there any follow-up requirements: e.g. counselling, legal, insurance related?



International Federation  
of Red Cross and Red Crescent Societies

**CRITICAL INCIDENT MANAGEMENT  
IFRC CONTRY CLUSTER OFFICE  
FOR ARGENTINA, BRAZIL, CHILE, PARAGUAY & URUGUAY**

A post incident report is to be produced and forwarded to senior management.

It is absolutely necessary to ensure support is provided to those directly affected and those closely involved with the situation.

For any other assistance, reports and recommendations please don't hesitate to contact. The undersigned.

-- INITIAL SIGNED --

Alexandre Claudon de Vernisy  
Head of Country Cluster Office  
for Argentina, Brazil, Chile, Paraguay y Uruguay

INITIAL