



**GLOBAL
INITIATIVE**
AGAINST TRANSNATIONAL
ORGANIZED CRIME

CRITICAL INCIDENT MANAGEMENT PROCEDURE

2024

CONTENTS

Introduction.....	2
Why does the GI-TOC have this procedure?	2
When is this procedure used?	3
Activation triggers	3
Principles	4
Team structure	5
Composition notes	5
Phases	7
Resources	7

INTRODUCTION

The GI-TOC recognizes the importance of responding to critical incidents that affect GI-TOC team members and the organization. As such, this procedure details how the GI-TOC defines critical incidents, the principles and phases that are followed when responding, the team structure and composition, and the resources that are used to support the management and response to critical incidents.

WHY DOES THE GI-TOC HAVE THIS PROCEDURE?

If a critical incident occurs, the GI-TOC will form a critical incident management team (CIMT) as illustrated in depth below, and use this procedure to:

- Prevent (further) harm and ensure the health, safety and well-being of team members, who are direct victims of, or indirectly or otherwise affected by the critical incident.
- Assure the affected people, families of the affected people, other stakeholders and regulators of an adequate and effective response.
- Fulfill the GI-TOC's legal obligations and reduce the risk of litigation or liability.
- Safeguard the GI-TOC's information, assets, integrity, reputation and mission.
- Ensure effective organizational management and business continuity.

WHEN IS THIS PROCEDURE USED?

This procedure is used when the GI-TOC is experiencing a critical incident, which is defined as:

An incident that has caused, or has the potential to cause, critical harm; and/or an incident that the affected person(s) believe the critical incident management team should be activated to manage.

And thus, requires additional leadership, coordination, resources and focus outside of normal line management structures to manage its impact and aftermath (through activating the critical incident management team).

The GI-TOC recognizes that this definition gives broad parameters for when a limited incident should be escalated to critical incident status. As such, it is preferred to activate the CIMT where there are uncertainties and then stand it down if required, rather than let an incident play out until it gets to a point where it can be defined as a critical incident.

Activating the CIMT is not an option of 'last resort', because it provides the GI-TOC with the opportunity to demonstrate that the organization is willing and able to provide support and reassurance to stakeholders and affected people under the GI-TOC's duty of care.

Activation triggers

If any one of the following trigger events occurs, the GI-TOC will automatically activate the CIMT:

- An affected team member requests the CIMT to be activated.
- An affected team member experiences critical harm, including death, threat to life or personal safety, sexual harassment or violence, major injury, kidnap, detention, harm to mental health, or other serious impacts.
- Major operational disruption to the GI-TOC, our partners, fellows or grantees.
- Major loss of assets or finance.
- Loss or breach of data/information.
- Misinformation/disinformation incidents.
- Significant challenge to the GI-TOC's integrity, reputation and mission.
- Regulatory investigation.
- Legal action against the GI-TOC.

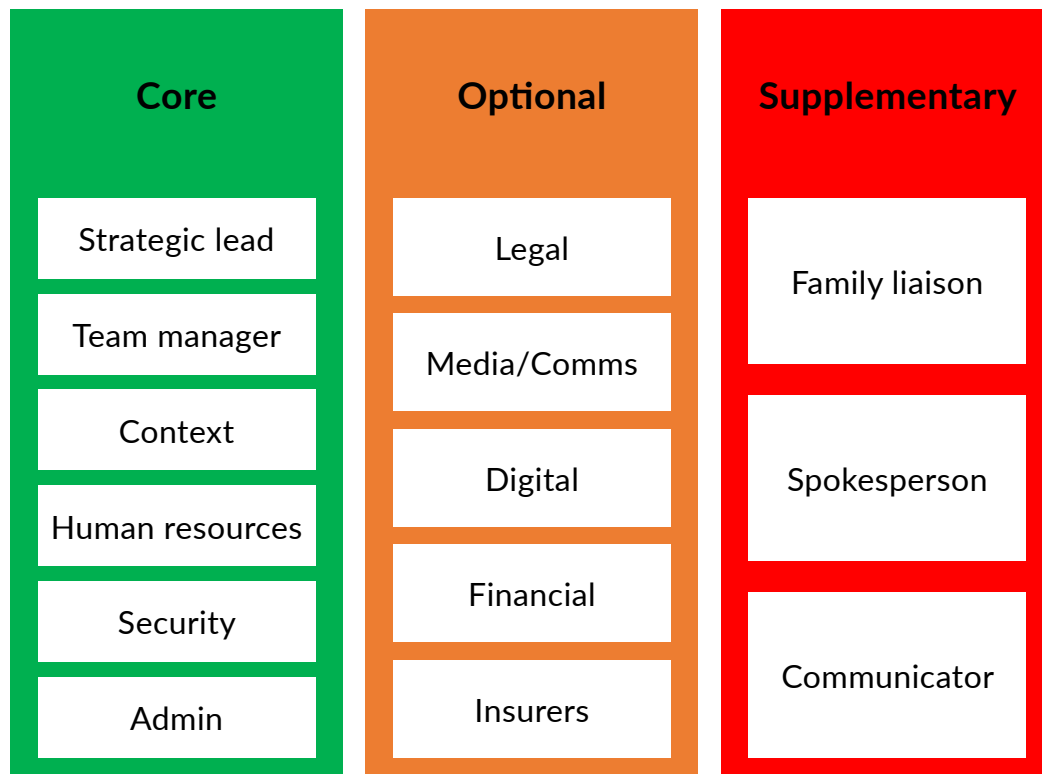
PRINCIPLES

The GI-TOC is committed to providing comprehensive critical incident support through the following principles and practices:

Principle	Description
Primacy of life	While the GI-TOC will safeguard the ability to continue to pursue its mission and protect its reputation, finances and resources, this will never be more important than the GI-TOC's efforts to preserve the lives of team members.
Context informed	The GI-TOC will work with team members, partners, fellows and/or grantees who are closest to the incident to ensure that critical incident responses are guided by local and specialized knowledge.
Person centered	Where practicable, the GI-TOC will ensure that affected team members have full input into the CIMT's decision making.
Available	The GI-TOC will always respond to critical incidents in a timely manner and provide continuous management until their resolution. This is achieved through incident reporting, this procedure and assigning primary and alternative representatives to each CIMT role.
Capable	The GI-TOC will ensure that it has the capability to manage critical incidents by identifying experienced and willing people for each CIMT role. These people will all attend regular CIMT training.
Resourced	The GI-TOC will ensure that it has adequate financial and human resources in place to respond to critical incidents. This includes maintaining relevant insurance and relationships with external responders.
Confidential	The GI-TOC will uphold strict confidentiality, communicating only to the stakeholders who can help to resolve the critical incident, or those that it is required to do so, by law. The GI-TOC does this because it understands the sensitivity and criticality of information in these situations.
Honest	The GI-TOC will honestly and effectively communicate with those involved in or affected by critical incidents. This includes team members, their families and all other relevant stakeholders, including regulators. However, this principle may not be applied to abductors and other adversaries when this is appropriate in resolving the incident.

TEAM STRUCTURE

The CIMT is a cross-functional team in the sense that several different skill sets are required to effectively reduce the impact of a critical incident. Where resources are limited, the CIMT can comprise team members and external consultants or stakeholders. The CIMT is composed of three teams, as shown below:



Composition notes

- The strategic lead acts as the person ultimately responsible for the management of the critical incident and has the final say in any decisions.
- The team manager has functional authority over all other team roles and makes the decisions regarding who is needed on the team and for how long.
- CIMT members are selected based on relevant skills, experience and personality, rather than seniority.
- Each CIMT role has a primary and alternative person, to allow for holidays, absences, operational demands and unforeseen circumstances, where possible.
- In some circumstances, the same person may be required for more than one role.

Core roles are required for every single critical incident.

Role	Responsibilities
Strategic lead	Retains ultimate responsibility for decisions; provides regular situational reports to key stakeholders; ensures team manager implements decisions; makes initial contact with families, connecting them to family liaison.
Team manager	Acts as key advisor to the strategic lead, ensuring decisions are taken with a 'wider perspective'; considers the implications of each decision; manages all team roles (except the strategic lead).
Context	Advises on local context and/or programmes; ensures CIMT decisions are contextually appropriate; liaises with external stakeholders in the region/country.
Human resources	Advises on HR policy and contractual obligations; coordinates family liaison; coordinates medical and well-being support, monitors health and well-being of the CIMT, advising when rest should be taken.
Security	Advises on any safety and security implications; builds scenarios and possible outcomes; liaises with external security providers (where required).
Admin	Records all information, communication and decisions; provides administrative support to the CIMT.

Optional roles have a specialist focus and are activated as dictated by the critical incident.

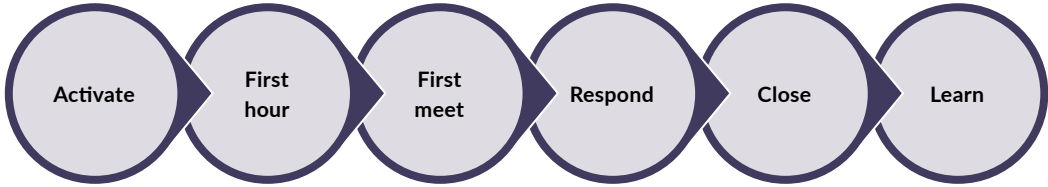
Role	Responsibilities
Legal	Reviews duty of care obligations; informs strategic lead and team manager of obligations and recommendations; connects to local legal representation.
Media/Comms	Scans the media for specific information; manages media relations and external statements; manages internal communications; provides guidance to families regarding handling the press.
Digital	Guides internal information and digital security; supports the response to information and digital security incidents.
Financial	Ensures adequate financial resources are available; implements financial transfers (where required).
Insurers	Confirm policy cover, provide advice around critical incident responses, scenarios and potential outcomes, connect to responders.

Supplementary roles have a specialist focus and are activated as dictated by the critical incident and do not attend CIMT meetings.

Role	Responsibilities
Family liaison	Communicates between the CIMT and families; keeps families informed of how the GI-TOC is managing and resolving the critical incident; assists in establishing the needs of families and then connecting them to appropriate support.
Spokesperson	Acts as the GI-TOC's external-facing representative during planned media releases or press conferences.
Communicator	Communicates between the CIMT and abductors; informs the CIMT of abductors demands, informs the abductors of the CIMT's demands.

PHASES

The CIMT adopts a phased approach to managing critical incidents. This helps them to identify specific actions at each phase. The phases are as follows:



RESOURCES

This procedure is supported by several resources that are used to support the management and response to critical incidents, as follows:

Resource	Description
Role descriptions and phase actions	<ul style="list-style-type: none">■ The role descriptions remind each CIMT member of their role-specific actions in each phase.■ The phase actions remind all CIMT team members of the combined actions in each phase, providing tips and considerations.
Dashboards, logs, contacts and scenarios	<ul style="list-style-type: none">■ The dashboards provide an up-to-date picture of the CIMT's work and objectives at and after the first hour phase.■ The logs record each event and major decision, triggering actions at specific times.■ The scenarios provide a systematic method to develop responses to the best, worst and most likely scenarios.



GLOBAL INITIATIVE

AGAINST TRANSNATIONAL
ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 600 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net