GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

INCIDENT REPORTING PROCEDURE

2024

CONTENTS

INTRODUCTION

The GI-TOC recognizes the importance of responding to GI-TOC team members who have been affected by or witnessed an incident. As such, this procedure details the GI-TOC's approach to incident reporting, defining why it is important to report incidents, what an incident is and how to report, escalate and follow up on incidents.

This procedure does not include the reporting of safeguarding incidents (including sexual harassment, sexual exploitation, bullying and abuse), which should be reported under the GI-TOC's whistle-blowing policy, available in the Operations manual.

WHY DO WE REPORT INCIDENTS?

All incidents and near misses that impact on those working on behalf of the GI-TOC must be reported to a tether or supervisor. This is important because it:

- Ensures that **immediate support** can be provided to the affected person(s) to reduce any remaining risks to them or others.
- Ensures that **hibernation**, **relocation** and/or **evacuation** and other support can be properly considered and/or provided.
- Allows the GI-TOC to identify any **trends** or **patterns** of incidents team members or the organization are exposed to and to determine whether any remedial action to prevent future recurrence of similar incidents is warranted or whether the security environment in a given location is deteriorating or improving.
- Provides the GI-TOC with a **measurable indicator** of whether existing policies and procedures are sufficiently reducing risk or whether alternative approaches require exploration.
- Ensures that the GI-TOC **continues to learn** from past incidents that have been reported and managed.

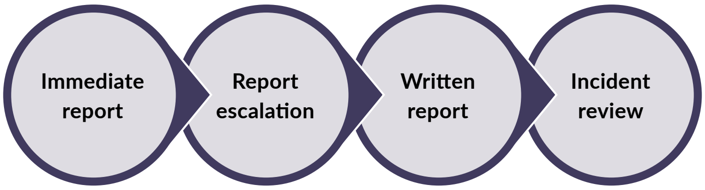
WHAT IS AN INCIDENT?

The following table details threats that the GI-TOC considers to be incidents. Please bear in mind that this is not an exhaustive list. If there is any confusion about what constitutes an incident, report it anyway. Any incident that occurs either at work or outside of work should be reported.

Incident affecting	Example threats
Those **working on the GI-TOC's behalf**	▪ Abduction/kidnapping ▪ Abuse-of-power situations ▪ Ambush ▪ Arrest and detention ▪ Bombing/IED ▪ Carjacking ▪ Checkpoints ▪ False flag/imposter incidents ▪ Landmine accidents ▪ Natural disasters and diseases ▪ Personal attack or assault and attempted assault ▪ Physical surveillance of team ▪ Threats of harm (made in any format) ▪ Traumatic or highly stressful events ▪ Vehicle accidents and incidents ▪ Workplace accidents that cause physical or mental harm or injury ▪ 'Near-miss' incidents ▪ Any other situation that causes physical or mental harm or injury.
The GI-TOC's **information security**	▪ A malware infection ▪ Ineffective security controls ▪ Information or system access violations ▪ Lost or stolen portable storage media or other computing equipment ▪ Malfunctions of hardware or software ▪ The exposure of personal or private information ▪ Uncontrolled system changes
The GI-TOC's **finances or assets**	▪ Bribery or attempted bribery ▪ Extortion or attempted extortion ▪ Theft of funds ▪ Theft or deliberate damage of equipment and other property
The GI-TOC's **reputation**	▪ Accusations from partners, grantees, fellows or other stakeholders in the GI-TOC's sector ▪ Negative accusations made in public ▪ Negative news stories ▪ Negative social media posts
The GI-TOC's **operations**	▪ Deteriorating security situation ▪ Disruption to the GI-TOC's projects/observatories due to insecurity ▪ Threatened or actual harm specifically targeted at the GI-TOC or the GI-TOC's partners
The GI-TOC's **policies**	▪ Non-compliance with any of the GI-TOC's policies or procedures

INCIDENT REPORTING PROCESS

To aid understanding, the diagram below is used to represent the incident reporting journey:



Immediate report

Any person who is working on the GI-TOC's behalf and affected by an incident, near-miss incident or witness to an incident that has caused or has the potential to cause harm to themselves or relevant others in the GI-TOC, must verbally inform their tether or supervisor **immediately and when safe to do so**. In most circumstances, a verbal report is ideal.

The tether or supervisor will want to quickly establish the facts about the incident and determine its severity for possible escalation. This is done by gaining the following information (in order):

- **WHO** is reporting the incident, and **WHO** has been involved?
- **WHERE** is the individual(s) involved in the incident reporting from?
- **WHERE** did the incident occur?
- **WHAT** has happened?
- **WHAT** actions have been taken so far?
- **WHAT** actions are going to be taken?
- **WHAT** further assistance is required?
- Does the affected person believe the GI-TOC's **critical incident management team** should be activated?

Report escalation

The tether or supervisor will then escalate the verbal report to specific people, depending on its category,[1] as follows:

Category	Definition	Escalation
Limited incident	An incident that has caused, or has the potential to cause, **limited harm**. And thus **does not require** additional leadership, coordination, resources and focus outside of normal line management structures to manage its impact and aftermath.	The tether or supervisor informs the relevant manager/ project manager.
Critical incident	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 tether or supervisor informs the relevant manager/ project manager and the director or deputy director.

Written report

Following the immediate report, it is the supervisor's responsibility to document the incident in an incident report form (in coordination with the affected person(s) and witnesses), **within three days**. A written incident report states exactly what happened (in as much detail as possible).

Key information in the written report will normally include:

- Who reported the incident, and when?
- What happened, where and when?
- Who was involved and what was the impact on those affected?
- What assets were lost or damaged?
- Was the GI-TOC or team members directly targeted during the incident?
- Were any of the GI-TOC's team members directly targeted because of any profile factors that resulted in their increased exposure to risk (e.g., gender, sexual orientation, gender identity, gender expression)?
- Were any weapons used?
- What were the immediate actions taken?
- Who has been informed?
- What are the implications for those involved?
- What further actions should be taken?

The incident may also need to be reported to others outside of the GI-TOC, including law enforcement, affected data controllers and data subjects, donors, relevant partners, suppliers and insurers.

Incident review

An incident review is **mandatory for critical incidents** and this process is defined in the critical incident management procedure and resources. For limited incidents, an incident review is not mandatory.

However, the affected person(s), the tether, supervisor, project manager, security committee and the director or deputy director can request that an incident review is conducted with relevant persons. This should ideally be **within seven days** of the incident and no later than three weeks after the incident.

Discussing the incident as a group will enable facts to be confirmed and changes in procedures to be discussed. Care should be taken if the incident involved any events that the affected person(s) found, or could have found, traumatizing. As such, the incident review should not focus on discussing any feelings related to the incident or delve deeply into any traumatic material. If the affected person(s) express concerns about their or others' psychological well-being, they can be referred to relevant support services for further assessments and care.

NOTES

1 If the tether is unsure of the incident category, they should treat it as a critical incident.

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