GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

SAFETY AND SECURITY POLICY

2024

CONTENTS

Introduction 2

Security risk management framework 2

How to access the framework 2

Purpose 3

Review 3

Complementarity with other frameworks and codes 3

Policy 4

Duty of care 4

Non-compliance 4

Risk appetite 5

Inclusive security and increased exposure 6

Principles 7

Strategies 8

Responsibilities 8

Duty of care obligations 11

Relocation and evacuation 14

Annex 1 – Risk management methodology 16

Notes 19

INTRODUCTION

Security risk management framework

This policy is part of the GI-TOC Security Risk Management Framework, as illustrated below:

How to access the framework

The following provides **entry points into the framework** for specific tasks.

Task	Key document	Resources
I want to know our **policy positions**	This document	–
I want to **travel**	Travel guidance and procedure	■ Trip risk level tool ■ Travel registration and tracking form ■ Risk and contingency mission planner ■ Emergency contact information ■ Proof of life form
We have **resident team members**/need to develop a country security plan	Country management procedure	■ Country welcome pack ■ Country security plan ■ Country risk assessment
I've been affected by or witnessed an **incident**	Incident reporting procedure	■ Incident report form
We want to manage a **critical incident**	Critical incident management procedure	■ Role descriptions and phase actions ■ Dashboards, logs, contacts and scenarios ■ Informed consent and confidentiality agreement

Purpose

This policy details how the GI-TOC achieves its duty of care obligations. It applies to all those who work on the GI-TOC behalf, regardless of their location.

Review

To meet with sector best practice, risk management developments and any changes in applicable law, the GI-TOC agrees to review this policy and any documents that govern our security risk management every two years as a minimum. It is the responsibility of the Management team to oversee this review, with implementation in collaboration with other key internal stakeholders and, where appropriate, external third-party providers.

Complementarity with other frameworks and codes

Several frameworks guide the GI-TOC's programme and operations management and shape the GI-TOC's overall behaviour and approach to its work. This safety and security policy is complementary to several documents, including but not limited to:

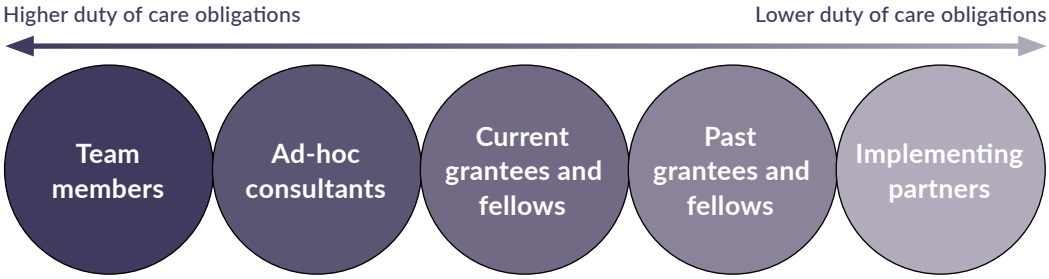
- Board and governance arrangements
- Statement of ethics of behaviour and key principles
- Code of conduct
- Travel policy
- Operations manual
- Guidelines for research
- Procurement policy
- Social media policy
- Equality and diversity policy
- Disciplinary procedure

POLICY

Duty of care

The GI-TOC takes the safety, security and well-being of those working on its behalf very seriously and fully accepts its duty to provide a reasonable standard of care to them and to take reasonable steps to mitigate foreseeable harm.

The GI-TOC has different duty of care obligations to different categories of people ('duty bearers') who work on its behalf based on the nature of the relationship with them, as detailed below in the duty of care obligations section. The following graphic illustrates the spectrum of the GI-TOC's duty of care obligations for these different duty bearers.



The security of those working on the GI-TOC's behalf shall remain a higher priority than the protection of material assets, the preservation of programmes, the expression of advocacy objectives or the protection of the GI-TOC's reputation.

The GI-TOC's duty of care is exercised through the application of the safety and security policy and other management policies and procedures. The systems developed to manage duty of care include, but are not limited to, informing team members about work-related risks, preparing team members to manage and treat risks, managing risks effectively according to GI-TOC policy, managing limited incidents and critical incidents when they occur, and seeking to ensure ongoing, post-incident care and is available to team members.

Non-compliance

Any deliberate breach of this policy or any other element of the safety security risk management framework is considered a disciplinary matter and may result in disciplinary action, up to and including termination of contract, in a manner that follows the GI-TOC's disciplinary procedures and the required legal framework. However, the GI-TOC will also take a discussion-first approach so that there is a suitable space to assess the appropriateness of security measures and identify improvements to this framework and any standard operating procedures.

Risk appetite

Background

The GI-TOC's mission, programmes and operating locations inherently involve exposure to insecurity and the risk of violence because we work at the front line of the fight against organized crime, and illicit trafficking and trade. As such, the GI-TOC purposefully follows a risk management (not risk aversion) approach, where staff safety and security are paramount. The GI-TOC's appetite to take risk will always take account of its strategic objectives and mandate, as well as the impact of other strategic factors (e.g., programme criticality and impact of key relationships).

Achieving the GI-TOC's risk appetite

The GI-TOC ensures that it does not mistakenly operate above its risk appetite, by having clear organizational and operational risk thresholds, using measurable indicators (present in its risk assessments) and ensuring that risk decisions are escalated to appropriate level. See Annex 1 for a detailed explanation of our risk management methodology.

Organizational risk threshold

The GI-TOC as an organization will not seek to work, or continue to work, in areas where the residual risk is assessed as **HIGH**, or **VERY HIGH**, unless there is a critical reason to do so. Residual risk identified as **VERY HIGH** is escalated to the Board at the time of the risk being identified.

Operating above organizational risk threshold

If the GI-TOC decides to accept risks that are higher than its organizational risk threshold, it will always take account of the strategic relevance and criticality of the work. This includes assessing the impact to those involved and the GI-TOC's capacity to respond should an incident occur. The decision to operate above the GI-TOC's organizational risk appetite must be taken by the Management team. Risks identified as **VERY HIGH** are to be escalated to the Board at the time of the risk being identified. The director will inform the Board if we exceed our organizational risk threshold.

Operational risk threshold

The GI-TOC observatories, programmes and operations have the freedom to work below the operational risk threshold. Where the residual risk is assessed as **MEDIUM**, **or above**, they are escalated to the Management team for discussion around the risks, mitigations, alternative and lower risk ways of achieving the same impact, and either approve, or decline.

Individual risk appetite

The GI-TOC recognizes that there may be a difference between the organization's risk appetite and individual's risk appetite. As such:

- Risk appetite is **discussed with team members at their recruitment/engagement** to ensure that they have understood the risk profile of the work they will undertake with the GI-TOC and mutually agree to appropriate levels of organizational and individual risk appetite.

- Where team member(s) have a **lower risk appetite** than the GI-TOC, the team member(s) are able to discuss and (if appropriate) agree not to pursue activities on behalf of the GI-TOC that are not commensurate with the mutually agreed risk appetite. However, if the risks are constant, frequent, or long-term, the GI-TOC will undertake a review to determine an appropriate course of action, which could include an assessment as to whether employment or engagement should continue in its current form.
- Team member(s) with a **higher risk appetite** than the GI-TOC must work within the GI-TOC's risk appetite.

Trip risk levels

The GI-TOC uses five trip risk levels to help understand and manage risk exposure during travel:

VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH

Inclusive security and increased exposure

The GI-TOC's risk management is inclusive and non-discriminatory. It seeks to ensure that mitigations result in (to the extent possible) equal and fair protection for all. While mitigations may sometimes appear unequal, the intended outcome is to arrive at the same level of acceptable risk.

The GI-TOC recognizes that the profile of an individual, their work with the organization, and the context that they work in can all contribute to their increased exposure to risk. In recognition of this, the organization seeks to identify, assess and mitigate these risks as part of the GI-TOC's daily operations and systematically through its risk assessments, travel process and country security plans.

The following table identifies some example factors that can result in an increased exposure to risk:

Individual	Organizational	Contextual
■ Age ■ Sex and gender ■ Sexual orientation, gender identity, gender expression ■ (Dis)ability ■ Physical/mental health status ■ Physical appearance and clothing ■ Trauma history and/or previous history of being involved in security incidents	■ Seniority/hierarchical position ■ Role/responsibilities ■ Contract type ■ Contract duration ■ Travel obligations ■ Accommodation ■ Creating, receiving and sharing sensitive information ■ Interactions with vulnerable communities (type and frequency)	■ Legal (national laws and their enforcement, including lack of protections) ■ Rural, urban, regional differences ■ Social and cultural beliefs and practices ■ Religious and other beliefs and practices ■ Level of acceptance for the GI-TOC's work by its stakeholders, contextual actors and the security environment

Individual	Organizational	Contextual
■ Nationality/national origin ■ Ethnicity ■ Religion ■ Marital/partnership status ■ Education status ■ Socio-economic status ■ Attitudes and behaviours ■ Political membership/ affiliation/activity ■ Previous professional experience ■ Previous or current employers	■ Relationship with external actors ■ The GI-TOC's culture and mission	

The GI-TOC also recognizes that individuals may not wish to be public with some of their profile factors (e.g., sexual orientation, gender identity, gender expression). As such the organization provides guidance to all individuals around these specific profile areas.

Principles

The following principles orientate the GI-TOC's security risk management:

Principle	Description
Do no harm	When assessing the risks for those who work on the GI-TOC's behalf, the organization is cognisant of the risks to others and **seeks to minimize the harm** it may be inadvertently doing simply by being present, providing support, or asking people to represent its mission.
Primacy of life	While the GI-TOC will safeguard its ability to continue to pursue its mission and protect its reputation, finances and resources, this will never be more important than its efforts to **preserve the lives** of those who work on the GI-TOC's behalf.
Shared responsibility	GI-TOC staff are all responsible for and should be actively engaged in their safety, security and well-being, including reporting incidents. This is the case for **strategic**, **operational** and **individual activities**. Any failure at any level, constitutes a failure of all levels.
Well-being	The well-being of those who work on the GI-TOC's behalf is paramount. The GI-TOC will provide team members with access to **appropriate medical and psychological care** and rest. This includes those affected by incidents and managing the response to incidents.
Freely decline	The GI-TOC actively shares information about the risk that those who work on its behalf may face so that they can make an informed decision to either consent to these or (if appropriate) agree **not to pursue activities** on behalf of the GI-TOC that are not commensurate with the mutually agreed risk appetite.[1]
Continuous improvement	The GI-TOC provides **assessment**, **reflection and feedback mechanisms** to inform any improvements it can make to its security risk management practices.
Partnership	The GI-TOC respects the **agency of its partners**, **grantees**, **fellows** and others that it works with. The organization ensures that they are informed of risks to the GI-TOC, sharing collective mitigations that arise from its activities, but it does not enforce the GI-TOC's risk appetite on them.

Strategies

As the locations that those who work on the GI-TOC's behalf visit and work in present different risks that originate from different threats, the organization will assess and deploy different security risk management strategies in each location. The GI-TOC recognizes that different security strategies can, and should, be deployed at different times and with different weightings.

However, the GI-TOC always prefers employing non-violent, peaceful strategies and **does not use armed deterrence** strategies, violence or weapons of any kind. Below is a list of the strategies that it may choose to deploy:

Strategy	Description
Low profile	Reducing risk by **remaining under the radar**.
Acceptance	Reducing risk by **gaining acceptance** for the GI-TOC's work.
Physical protection	Reducing risk through **physical protection measures** *(e.g., walls, locks, window bars).*
Non-armed deterrence	Reducing risk or responding to an incident by **containing the threat** with a non-armed counter-threat *(e.g., CCTV, legal action).*
Network leverage	Reducing risk or responding to an incident by **leveraging** state and non-state allies to positively influence spoilers.
Protective advocacy	Reducing risk or responding to an incident by **raising awareness** of an individual or organization at risk with the media *(e.g., creating a high-profile campaign).*

Responsibilities

Strategic

Responsibility	Responsible
Hold ultimate accountability for the Duty of care of all those who work on the GI-TOC's behalf	Director
Ensure adequate internal financial and human resources to support the management of safety and security risk	Management team
Agree any changes to the GI-TOC's risk appetite	Board
Approve situations where the GI-TOC decides to accept risks above the GI-TOC's risk appetite	Management team
Review and approve the strategic risk assessment on an annual basis	Leadership team
Review and approve strategic risks on an annual basis	Director
Maintain, monitor and improve the security risk management framework	Director

Operational

Responsibility	Responsible
Postpone or suspend any activities where the risks have escalated beyond the GI-TOC's operational risk appetite	Management team
Close observatories or operations where the risks have escalated beyond the GI-TOC's operational risk appetite	Management team
Approve the opening of new countries	Management team
Review the observatory risk assessments and security guidelines	Observatory
Approve the observatory risk assessments and security guidelines	Management team
Review limited incidents	Observatory/Security lead
Review critical incidents	Management team
Ensure adequate travel, accident, crisis response and other relevant insurance is in place	Management team
Agree safety and security training requirements	Management team
Provide technical security guidance, support and advice to those who work on the GI-TOC's behalf	Head of critical incident management team
Coordinate with external providers (e.g., insurance providers, travel management companies and risk management consultancies) to ensure adequate technical expertise	Director of human resources
Review and approve or decline all domestic and international travel to **VERY LOW**, **LOW** and **MEDIUM** trip risk levels	Line manager
Review and approve or decline all domestic and international travel to **HIGH** and **VERY HIGH** trip risk levels	Management team
Authorize medical and security related domestic relocations and international evacuations	Observatory or management team

Line managers

- Ensure their team members have access to security policy and procedures.
- Manage risks and respond to limited incidents.
- Monitor team member compliance to security policies, plans and procedures.
- Report and escalate security incidents, as per the incident reporting procedure.
- Identify team members' security training, learning and development needs, and ensure access to the training (including appropriate planning and resourcing).

Team members

- Carefully read, get acquainted with, and fully comply with this security policy, the observatory security guidelines and all other documents that govern and regulate security risk management.
- Ensure that they have understood the risk profile of the work they will undertake with the GI-TOC and mutually agree to appropriate levels of organizational and individual risk appetite.
- Discuss and (if appropriate) agree not to pursue activities on behalf of the GI-TOC that are not commensurate with the mutually agreed risk appetite.[2]
- Will not increase risk exposure to the GI-TOC through their own personal political activities,

including campaigning, lobbying or public representation.

- Work with their line managers to manage risks and be responsible for taking reasonable and meaningful actions to manage their own safety and security.
- Follow security instructions to avoid unnecessary risks and prevent behaviour that brings themselves or others into danger.
- Participate in and contribute to organizational risk measures and be conscious of security conditions and risk.
- Understand that their individual behaviour is key to their own safety and security as well as that of their co-workers and the GI-TOC.
- Notify their line manager of any intention to travel, at the earliest possible opportunity.
- Request further information concerning any risk if they feel that they are not fully informed.
- Complete required security training.
- Ensure that emergency/next of kin contacts are up to date.
- Always be reliably contactable when travelling and inform their line manager of their location and other reasonably requested information at the pre-defined times in accordance with observatory risk assessment and travel procedures.
- Act responsibly to ensure personal and other information is used, shared, stored or disposed of appropriately, and must have regard to relevant regulatory requirements.
- Be aware of the risks of sharing information and opinions on social media and other public sites, in addition they must follow sign-off procedures for sharing the GI-TOC's information publicly.
- Act as the first responder to any safety and security incidents (where trained and when present).
- Report any incidents to their line manager that have caused or have the potential to cause harm to themselves, others, or the GI-TOC as soon as possible and when safe to do so.
- Submit a written report to their line manager within seven days of an incident.
- Contribute to a review of any incidents that have directly affected them or that they were witness to.

Ad-hoc consultants, current and past grantees and fellows and implementing partners

- Ensure that they have understood the risk profile of the work they will undertake with the GI-TOC and mutually agree to appropriate levels of organizational and individual risk appetite.
- Discuss and (if appropriate) agree not to pursue activities on behalf of the GI-TOC that are not commensurate with the mutually agreed risk appetite.[3]
- Will not increase risk exposure to the GI-TOC through their own personal political activities, including campaigning, lobbying or public representation and connecting this to the GI-TOC.
- Understand that their individual behaviour is key to their own safety and security as well as that of their co-workers and the GI-TOC.
- Be reliably contactable and inform the GI-TOC of reasonably requested safety and security information.
- Act responsibly to ensure the GI-TOC related information is used, shared, stored or disposed of appropriately, and have regard to relevant regulatory requirements.
- Be aware of the risks of sharing information related to the GI-TOC and their opinions on social media and other public sites.

- Verbally report to the GI-TOC any incidents that have caused or have the potential to cause harm to themselves or the GI-TOC as soon as possible and when safe to do so.
- Contribute to a review of any incidents that have directly affected them, or they were witness to.

Duty of care obligations

The GI-TOC has different duty of care obligations to different categories of people ('duty bearers') who work on its behalf. This is reflected in how it implements this policy and the security risk management framework.

These duty bearers include the following:

- Team members (including pay-rolled staff, remote staff and long-term contractors when they are paid monthly for a period of 12 months or more).
- Ad-hoc consultants
- Implementing partners
- Current grantees and fellows
- Past grantees and fellows
- The GI-TOC's donors

For the GI-TOC's donors, the organization commits to:

- Understand the duty of care requirements that they place on the organization.
- Include funding requests in its proposals that finance meeting the GI-TOC's duty of care obligations.

For all other duty bearers, the GI-TOC commits to providing each duty bearer with the following, identified in the tables below.

Governance

Obligation	Team members	Ad-hoc consultants	Implementing partners	Current grantees/ fellows	Past grantees/ fellows
Conducting appropriate due diligence, prior to employment/contract/ engagement	✓	✓	✗	✓	✗
Fully communicating this policy and other relevant documents that govern and regulate risk and informing them of their risk management responsibilities (if relevant to their role)	✓	✓	✓	✓	✗
Providing access to threat and risk information	✓	✓	✗	✓	✗
Providing risk reduction measures when working with the GI-TOC	✓	✓	✗	Case by case	✗

Obligation	Team members	Ad-hoc consultants	Implementing partners	Current grantees/ fellows	Past grantees/ fellows
Internally ensuring/ externally encouraging the choice not to travel or pursue activities on behalf of the GI-TOC that are not commensurate with the mutually agreed risk appetite	Ensuring	Ensuring	Encouraging	Encouraging	✗
Informing of risk management responsibilities	✓	✓	✓	✓	✗
Managing their risk in their contracted location, during normal working hours, when engaged with the GI-TOC	✓	✓	✗	✗	✗

Travel

Obligation	Team members	Ad-hoc consultants	Implementing partners	Current grantees/ fellows	Past grantees/ fellows
Managing their risk when travelling at the GI-TOC's request outside their contracted location for the organization at all times	✓	✓	✗	✓	✓
Providing a verbal pre-departure briefing when travelling at the GI-TOC's request for HIGH or VERY HIGH trip risk levels or when requested by the traveller	✓	✓	✗	✗	✗
Providing a Proof of life form when travelling at the GI-TOC's request for HIGH or VERY HIGH trip risk levels, or when requested by the traveller	✓	✓	✗	✓	✗
Providing a reputable travel management company through which they can book travel, when travelling for the GI-TOC and at its request	✓	✓	Case by case	✓	✓
Ensuring access to (or information on) basic security and travel training when travelling for the GI-TOC at its request	Access	Information	✗	Information	✗

Obligation	Team members	Ad-hoc consultants	Implementing partners	Current grantees/ fellows	Past grantees/ fellows
Providing appropriate travel and personal accident insurance when travelling for the GI-TOC at its request	✓	✗	✗	✗	✗
Ensuring access to physical emergency medical care (and/or information) during travel/employment/ engagement	Access	Information	✗	✗	✗
Ensuring access to (or information on) appropriate counselling and psychological support before, during and after employment/deployment/ engagement, including post-incident	Access	Information	Information	Information	Information

Support and incident management

Obligation	Team members	Ad-hoc consultants	Implementing partners	Current grantees/ fellows	Past grantees/ fellows
Ensuring access to (or information on) critical incident response training	Access	Information	✗	Information	Information
Providing appropriate crisis response insurance	✓	✓	✗	Case by case	✗
Providing a facility for them to store their emergency contact information with the GI-TOC when travelling with us at our request	✓	✓	✗	✓	✓
Ensuring access to appropriate and specialized post-incident counselling and psychological support (for up to 6 sessions for one concern) in addition to the normal organizational provision	✓	✗	✗	Case by case	Case by case
Providing access to domestic security and medical relocation to those in their contracted observatory location as a result of a critical incident	✓	✗	✗	Case by case	✗
Providing access to international security and medical evacuation to those travelling outside of their contracted observatory location	✓	✗	✗	Case by case	✗

Obligation	Team members	Ad-hoc consultants	Implementing partners	Current grantees/ fellows	Past grantees/ fellows
Providing critical incident support during critical incidents	✓	Case by case	✗	Case by case	Case by case
Providing extensive critical incident management support as a result of a critical incident[4]	✓	✗	✗	Case by case	✗
Ensuring that they are fully aware that the GI-TOC cannot support them during a safety and security incident	✗	✓	✓	✓	✓

Relocation and evacuation

Through its Critical incident management team and procedure, the GI-TOC ensures appropriate mechanisms for relocation and evacuation. The support that the GI-TOC provides varies for each duty bearer, as described below.

Domestic security relocation and international security evacuation:

- The GI-TOC **is not obligated to** provide domestic security relocation and international security evacuation to ad-hoc consultants, implementing partners or past grantees and fellows.
- The GI-TOC **may** provide domestic security relocation and international security evacuation (as a result of a critical incident related to the GI-TOC) to current grantees and fellows on a case-by-case basis. The Critical incident management team would take this decision.
- The GI-TOC **does** provide domestic security relocation and international security evacuation (as a result of a critical incident related to the GI-TOC) to team members.

These decisions:

- Everybody has the right to request a review of their risk exposure in relation to security relocation or evacuation.
- Can be made by the Observatory lead or the Critical incident management team.
- Cannot be overruled by anyone unless the Critical incident management team determines that the security relocation would expose the individual(s) to greater immediate danger than remaining in the current location.
- Are binding for all affected persons. If they refuse to leave, they do so on the understanding that their contract is immediately terminated and that the GI-TOC no longer has any duty of care for them.

Where there is no possibility of relocating/evacuating everyone, affected persons who are deemed to be at the highest risk will be given priority and at the discretion of the Critical incident management team.

No one may return to a location after a domestic security relocation or international evacuation until a risk assessment has been fully completed, the identified security measures are/can be implemented, and following the approval of the Observatory lead and the Management team.

Domestic medical relocation and international medical evacuation

- The GI-TOC **is not obligated to** provide domestic medical relocation and international medical evacuation to ad-hoc consultants, implementing partners or past grantees and fellows.
- The GI-TOC **may** provide domestic medical relocation and international medical evacuation (as a result of a critical incident related to the GI-TOC) to current grantees and fellows, on a case-by-case basis. The Critical incident management team would take this decision.
- The GI-TOC **does** provide domestic medical relocation and international medical evacuation to team members.

These decisions:

- Can be made by the GI-TOC's insurers, or if not an insured evacuation, by an appropriately qualified and the GI-TOC nominated medical doctor.
- Are binding for all affected persons. If they refuse to leave, they do so on the understanding that their contract is immediately terminated and that the GI-TOC no longer has any duty of care for them.

Where there is no possibility of relocating/evacuating everyone, affected persons who are deemed to be at the highest risk will be given priority and at the discretion of the Critical incident management team.

No one may return to a location after a medical relocation/evacuation without written clearance issued by the GI-TOC's insurers or an appropriately qualified and GI-TOC nominated medical doctor.

ANNEX 1 – RISK MANAGEMENT METHODOLOGY

Introduction

Risk management is a means of identifying, assessing and controlling risks across an organization with a coordinated and cost-effective application of resources to minimize, control and monitor the likelihood and impact of adverse events, or to maximize the realization of opportunities. This annex explains the risk management methodology that the GI-TOC deploys. The GI-TOC follows a four-phase risk management process, detailed below:

Context

The context phase seeks to understand what the GI-TOC is trying to achieve in terms of mission and operational objectives. This is supported by a defined risk appetite.

- At an observatory level, this context is reviewed at the design and inception stage and at least annually throughout the life cycle.
- At the strategic level, the GI-TOC annually reviews this context and risk appetite.

Assess

The assess phase identifies, scores and applies strategies to threats and risks. In order to ensure that risks are effectively managed throughout the organization, the GI-TOC operates three levels of risk assessment, as follows:

- Travel risk assessment
- Country/observatory risk assessment
- Strategic risk assessment

The **likelihood** scoring that the GI-TOC uses is as follows:

Likelihood	Guideline
REMOTE	The risk will occur only in the most exceptional circumstances
UNLIKELY	The risk is not expected to occur in most circumstances
CREDIBLE	The risk will occur in some circumstances
LIKELY	The risk will occur in most circumstances
CERTAIN	The risk will occur in just about all circumstances

The **impact** scoring that the GI-TOC uses is as follows:

Level of impact	Loss of finance	Health of individuals	Ability to operate	Loss of reputation	Disruption to leadership
INSIGNIFICANT	Loss of < €10 000	Injury very unlikely. Short term illness, 1 week absence	No measurable operational delay or interruption/No effect on staff morale.	Negative reputations of consultants and their activities (who work on the GI-TOC's behalf)	Routine management time demands/ Observatories can manage independently
MINOR	Loss of between €10 000–€100 000	Minor injury, but no real impact on operations	Up to 1-week operational delay or interruption/Limited effect: no resignations of key staff	Perceived as being less reliable or a 'hard to work with' partner	Some demands on senior management time/Observatories can manage with support
MODERATE	Loss of between €100 000–€200 000	Severe or multiple injuries: short-term impact on operations sustained/ Psychological stress	Between 1 week and 1-month operational delay or interruption. Some appreciable effect: some resignations of key staff and/or discouraged recruitment/High turnover of staff	Perceived lack of impartiality and quality of reporting/ Critical review by a state with established ethics and morality	Significant demands on senior management time: limited disruption to normal business
MAJOR	Loss of between €200 000–€500 000	Many serious injuries/ Operational effectiveness compromised/ Permanent disability/ Long-term psychological injury	Between 1–2 months operational delay or interruption/ Significant effect: resignations of several key staff and/or discouraged recruitment/Cyber attack	Over 20% of reports perceived lack of impartiality and quality. Perceived lack of contextual understanding; acting irresponsibly; methodology and approach/Critical review by established academics or grouping of nation states/ Being sued	Very significant demands on senior management time: normal business disrupted
CRITICAL	Loss of > €500 000	Fatalities	More than 2 months operational delay or interruption/ Major effect: many resignations over sustained period and recruitment noticeably discouraged	Public accusations of negligence or hypocrisy	Overwhelming demands on senior management time: business dominated by this issue

The **risk** scoring that the GI-TOC uses is as follows:

		Likelihood				
		Remote	Unlikely	Credible	Likely	Certain
Impact	Critical	LOW	MEDIUM	HIGH	VERY HIGH	VERY HIGH
	Major	LOW	MEDIUM	HIGH	HIGH	VERY HIGH
	Moderate	VERY LOW	LOW	MEDIUM	HIGH	HIGH
	Minor	VERY LOW	LOW	LOW	MEDIUM	MEDIUM
	Insignificant	VERY LOW	VERY LOW	VERY LOW	LOW	LOW

Control

Operational risk threshold

The GI-TOC observatories, programmes and operations have the freedom to work below the operational risk threshold. Where the residual risk is assessed as **MEDIUM or above**, they will be escalated to the Management team for discussion on the inherent risks, possible mitigation measures and authorization.

Organizational risk threshold

The GI-TOC will generally not seek to work, or continue to work, in areas where the residual risk is assessed as **HIGH** or **VERY HIGH**, unless there is a critical reason to do so. Residual risks identified as **VERY HIGH** are to be escalated to the Board at the time of the risk being identified.

The control phase ensures that all risks are either reduced to below **MEDIUM** or (if they cannot) are escalated, as per above.

Monitor

The monitor phase ensures that after the completion of an initial assessment, each risk assessment is updated as indicated in the minimum standards. This process must include the following questioning:

- Are there any changes to the scoring of each risk?
- Are all the mitigations identified fully implemented?
- Are there any new threats that need to be added?

NOTES

1 However, if the risks are constant, frequent or long-term, the GI-TOC will undertake a review to determine an appropriate course of action, which could include an assessment as to whether employment, or engagement, should continue in its current form.

2 However, if the risks are constant, frequent or long-term, the GI-TOC will undertake a review to determine an appropriate course of action, which could include an assessment as to whether engagement, should continue in its current form.

3 However, if the risks are constant, frequent, or long-term, the GI-TOC will undertake a review to determine an appropriate course of action, which could include an assessment as to whether engagement, should continue in its current form.

4 Extensive critical incident management support refers to support beyond relocation, evacuation and medical assistance. Examples include the provision of family liaison services, financial support and extended leave.

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