GUIDE FOR INDEPENDENT ACCOUNTABILITY MECHANISMS ON MEASURES TO ADDRESS THE RISK OF REPRISALS IN COMPLAINT MANAGEMENT

A Practical Toolkit

Guide for Independent Accountability Mechanisms on Measures to Address the Risk of Reprisals in Complaint Management: A Practical Toolkit

Author:
Tove Holmström

Commissioned by the Independent Consultation and Investigation Mechanism (IDBG)

Editors:
Anne Perrault (UNDP-SECU), Ana María Mondragón, Pedro León and Victoria Márquez Mees (IDBG-MICI)

Design:
Alejandro Scaff

Cover photo:
Pexels

Back cover photo:
MICI

January 2019

MICI Independent Consultation and Investigation Mechanism

IAMnet Independent Accountability Mechanisms Network

FOREWORD

The idea of producing a toolkit that would assist independent accountability mechanisms (IAMs) address the risk of reprisals within the context of their complaint management process came as a result of discussions with members of the IAM Working Group on Retaliation. The Independent Consultation and Investigation Mechanism (MICI) commissioned Ms. Tove Holmström, an independent consultant, to research and generate a manual that would provide IAMs with general guidance, tools, and resources for addressing the risk of reprisals. The current document provides an array of alternatives for IAMs to learn about and use as relevant. As part of the process, Ms. Ana María Mondragón (former consultant at MICI), Ms. Anne Perrault (member of the United Nations Development Program accountability mechanism, SECU), Mr. Pedro León (consultant at MICI) and myself reviewed and provided guidance on the content. My appreciation to everyone for their contributions to this guide that will hopefully serve as an open knowledge resource to IAMs.

Victoria Márquez-Mees
MICI Director

Tove Holmström currently an independent consultant based in Paris, France is a former staff member of the UN Human Rights Office. Her work addresses business and human rights, with a particular focus on non-judicial grievance mechanisms. In this field, she has, amongst other, worked with the UN Special Rapporteur on the situation of Human Rights Defenders and the Organization for Economic Co-operation and Development before being commissioned to produce the IAMs toolkit. She is regularly consulted by development lending institutions and accountability mechanisms that are seeking to develop policies to better assess and address risks of reprisals against project stakeholders, complainants and other cooperating persons.

MICI, the Independent Consultation and Investigation Mechanism of the Inter-American Bank (IDB) Group, addresses environmental and social concerns from communities in the Latin American and Caribbean Region related to IDB financing.

For more information, visit www.iadb.org/mici

CONTENTS

ACRONYMS

CAO	Compliance Advisor Ombudsman (World Bank Group)
CERD	Committee on the Elimination of All Forms of Racial Discrimination
CIVICUS	World Alliance for Citizen Participation
CSO	Civil society organization
EHAHRDN	East and Horn of Africa Human Rights Defenders Project
EBRD	European Bank for Reconstruction and Development
EU	European Union
FIDH	International Federation for Human Rights
IAM	Independent accountability mechanism
IACHR	Inter-American Commission on Human Rights
IBRD	International Bank for Reconstruction and Development (World Bank Group)
IDA	International Development Association (World Bank Group)
IDB	Inter-American Development Bank
IFC	International Finance Corporation (World Bank Group)
IP	Inspection Panel (World Bank Group)
ISHR	International Service for Human Rights
IT	Information technology
LGBTI	Lesbian, gay, bisexual, transgender, and intersex
MICI	Independent Consultation and Investigation Mechanism (Inter-American Development Bank Group)
MIGA	Multilateral Investment Guarantee Agency (World Bank Group)
NGO	Non-governmental organization
OAS	Organization of American States
OHCHR	Office of the High Commissioner for Human Rights (United Nations)
OMCT	World Organization Against Torture
PBI	Peace Brigades International
PCM	Project Complaints Mechanism (European Bank for Reconstruction and Development)
PI	Protection International
SECU	Social and Environment Compliance Unit (United Nations Development Programme)
SLAPP	Strategic lawsuits against public participation
SOGI	Leadership Group on Sexual Orientation and Gender Identity (World Bank Group)
UN	United Nations
UPR	Universal Periodical Review

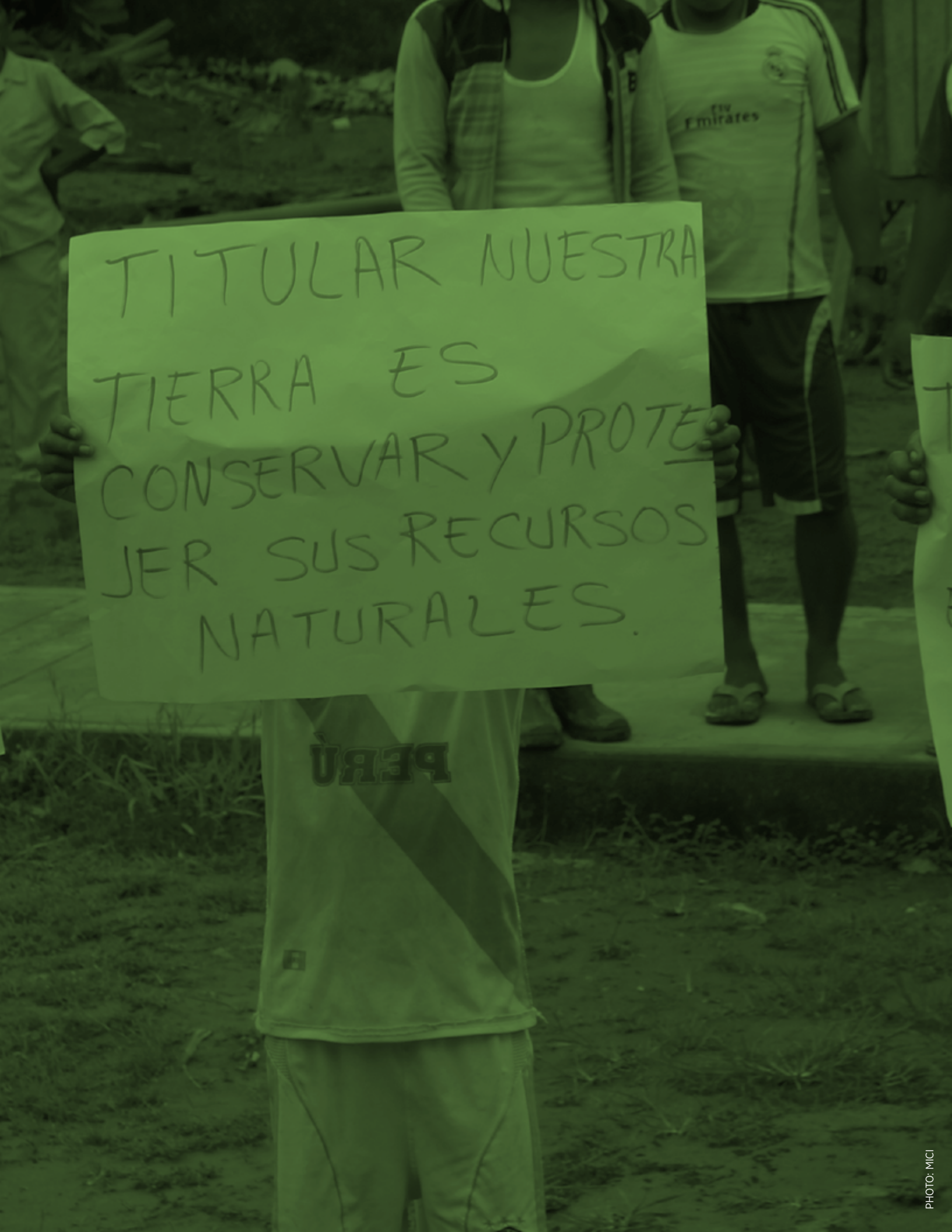

TITULAR NUESTRA
TIERRA ES
CONSERVAR Y PROTE
JER SUS RECURSOS
NATURALES.

PHOTO: MICI

INTRODUCTION

In recent years, reprisals[1] against those who bring complaints to independent accountability mechanisms, family members and others associated with them, have increased. Reprisals have also affected other related stakeholders, including consultants, interpreters, expert witnesses, and members of civil society organizations that have facilitated the IAM processes. These acts can not only devastate the lives of the individuals concerned and their families, but also have serious and deterrent consequences for the willingness and capacity of project-affected individuals and communities to use, and provide information to, the IAMs in the future. As such, reprisals have been identified by the IAMs themselves as a major challenge to their effective functioning.

This toolkit seeks to help IAMs approach the risk of reprisals, providing suggested actions, examples and tools that can be used to assess and address reprisals more efficiently and effectively.

Two key observations have underpinned the preparation of this toolkit: Reprisals in the context of IAM operations are likely to increase in the future, and, based on current global trends and patterns, are likely to evolve and intensify in terms of the forms they take and their gravity.

For several reasons, reprisals are likely to increase both in numbers and severity in the future. First, many of the IAMs' parent institutions are increasingly investing in transformative infrastructure projects, where risks of reprisal have been observed as particularly high.[2] Reprisals are also expected to increase given the current state of play for civil society, which is largely characterized by a rapidly deteriorating security environment for activists, journalists, and human rights defenders in general.

Current global patterns suggest that IAMs need to be prepared for a wide range of forms of reprisals, including public smear campaigns, digital surveillance, and the use of laws to punish and discredit complainants and those supporting them to bring their cases to the IAMs. Tragically, the reported spike in numbers of assassinations of individuals working to address land and environmental impacts, and of their next of kin, is also likely to be felt in IAM operations.

The toolkit has sought to understand the challenges IAMs currently face to prevent and address reprisals. IAMs typically intervene at a late stage of the project cycle at which reprisals may already be taking place. This points to the usefulness of a broader institutional approach to preventing and addressing reprisals, including during project design and implementation.

Another challenge relates to the limited mandates of the IAMs – they are not enforcement

1 - This toolkit uses the term "reprisal," which is understood to include intimidation, threats, harassment, punishment, judicial proceedings or any other retaliatory acts against requesters, complainants, and others associated with them or with the IAM process. Other terms commonly used by human rights mechanisms to address retaliatory acts (against individuals or groups that have sought to cooperate with them) include sanction, reprimand, and retaliation.

2 - Risks of reprisal in land sectors are particularly high. Concerns over these risks find support in a recent report by the UN Special Rapporteur on the situation of human rights defenders that raised alarm over the high number of assassinations of human rights defenders working on land and environmental rights. By way of illustration, according to the Special Rapporteur, in 2015, 185 individuals defending land and environmental rights lost their life across 16 countries. The sectors of mining and extractive industries (42 killings), agribusiness (20), hydroelectric dams and water rights (15), and logging (15) were major drivers of the killings.

mechanisms, and they cannot physically protect or otherwise directly safeguard people from the possible negative consequences of their engagement with the IAMs. Given these limitations, the toolkit focuses on preventative measures as the most appropriate means to counter risks and identifies other entities that can help prevent and respond to reprisals.

This toolkit has been prepared based on the assumption that risks of reprisal to requesters (those who submit a request to the IAM for an accountability process), and other related stakeholders can never be fully eliminated. Many individuals and groups seeking the intervention of IAMs are often already publicly pursuing human rights advocacy in their countries and are at high risk of reprisal because of that. As such, the risks they face for this work and those they face for engaging with IAMs are easily blurred. Nevertheless, accessing IAMs may aggravate existing risks. In this regard, it has been noted that ensuring the protection of requesters and others associated with them or the IAM process is a shared responsibility of the State(s), borrowers and other recipients of funding, parent institution clients and sub clients, the IAM(s) and their parent institution(s), the possible victims, and any other actors that can positively or negatively influence the safety of those at risk.[3]

Measures that will best address the risks of reprisal in each situation will depend on a range of factors. Such factors include the political and security environment, the source of the threat, the vulnerabilities and capacities of the individuals at risk to prevent and respond to the threats, the commitment of the project implementing agency and national authorities to address risks, and the capacity and willingness of the IAMs' parent institutions to engage with the source of the threat or with others that can influence the situation. There is therefore no blueprint or best model for reducing risks, and the unique circumstances of each case should determine the most appropriate response. Nonetheless, IAMs can take several baseline measures to reduce general risks against requesters, complainants, and other cooperating persons, as the toolkit suggests.

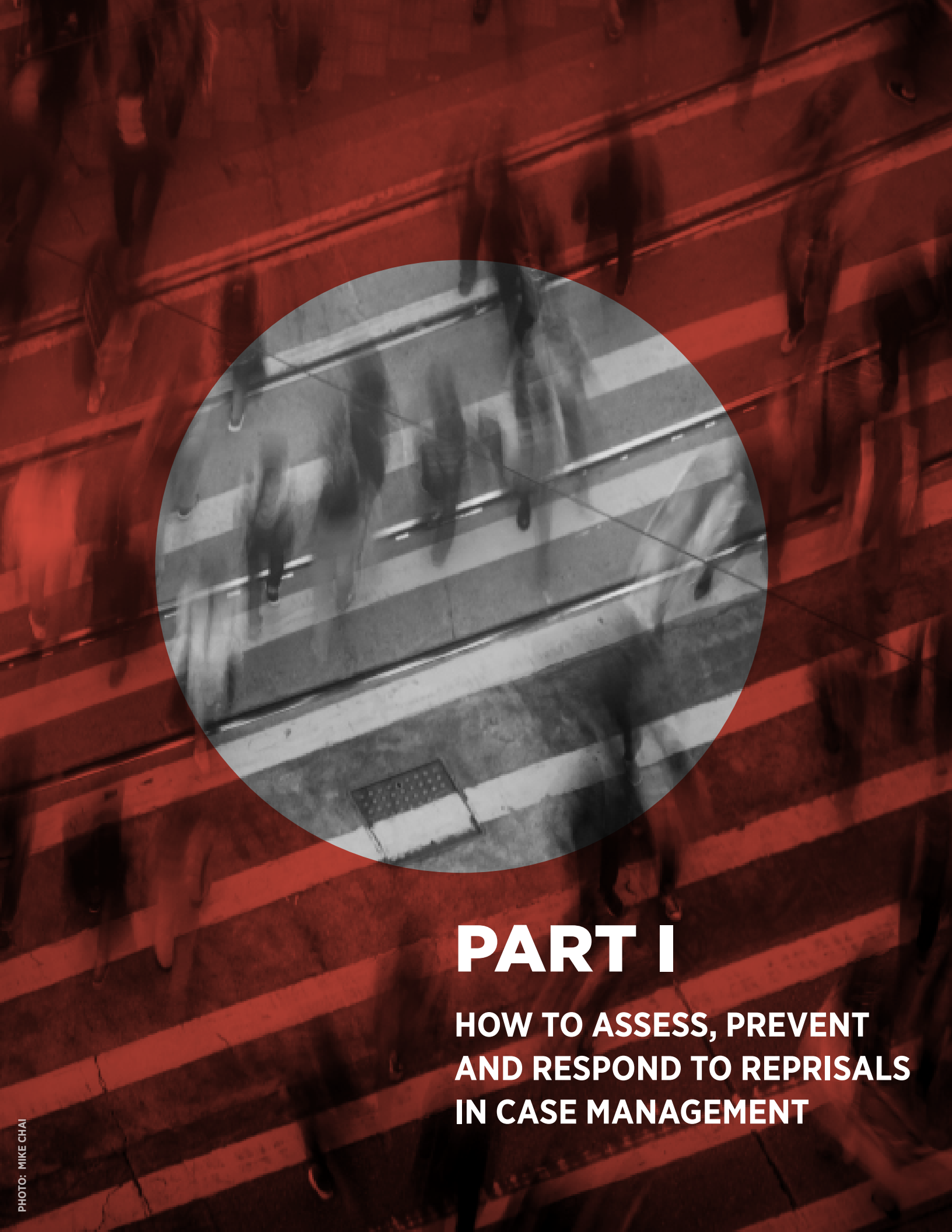
The toolkit has two parts. Part I focuses on how IAMs assess, prevent, and respond to reprisals, providing a series of actions they can consider to prevent and respond to reprisals as part of their complaint management process. These actions relate to understanding the risk context, developing strategies to reduce identified risks, and establishing protection timelines when reprisals are imminent or have occurred. Part 2 explores ways to strengthen the institutional capacity to prevent and respond to reprisals, focusing on actions the IAMs and their parent institutions can take, at the institutional level, to assess and address risks of reprisals.

Each suggested action is accompanied by practical support – the "tool" that can be deployed. This practical guidance includes examples of how an action (or tool) has been pursued by other IAMs or in other contexts, as well as templates, sets of questions that might be useful to consider, relevant resources, and organizations that can be approached for support.

The members of the IAM Network operate with different mandates, have different structures and have adopted, or are considering, different approaches to addressing reprisals. Therefore, some of the suggested tools may be more appropriate for some of the IAMs than others.

Available support for addressing reprisals will evolve over time. In this regard, this toolkit should be considered a "living" document to which each IAM and other actors can continue to contribute information about reprisals, including successful approaches to addressing them.

3 - See UN Office of the High Commissioner for Human Rights: Revised Manual for Human Rights Monitoring (Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons) for a discussion on the shared responsibility to protect.



PART I

HOW TO ASSESS, PREVENT AND RESPOND TO REPRISALS IN CASE MANAGEMENT

PHOTO: MIKE CHAI

ASSESSING THE LEVEL OF RISK

An important first step in the process of addressing risk of reprisals in the context of IAM cases is to assess – as far as possible – the probability of reprisals against requesters and other cooperating persons, and the severity and impact of those reprisals.

For that purpose, this toolkit presents four actions, while underscoring the fact that alternatives might be available.

ACTION 1: CONDUCT A REPRISALS RISK ASSESSMENT

What it is

A reprisals risk assessment should consider the likelihood that retaliatory acts will occur, and the capacities of the victims to reduce this likelihood and effectively respond to such events.

Risks of reprisal will be unique for each IAM case, and will differ according to many factors, including the degree of impunity in the country, the profile and location of activities, and the vulnerabilities and capacities of the individuals concerned to prevent and respond to reprisals. It should be noted that reprisals rarely involve one single action, but rather a series of reprisals over time.

Why it is important

Understanding the risk context is a prerequisite for the IAMs to be able to design and implement effective measures that can reduce risks of reprisal. Assessing risk might seem daunting at first, but once it is done systematically it becomes part of the case management process.

Examples

The Inspection Panel (IP) of the World Bank Group's International Development Association (IDA) and International Bank for Reconstruction and Development (IBRD) and the Compliance Advisor Ombudsman (CAO) of the World Bank Group's International Finance Corporation (IFC) and Multilateral Investment Guarantee Agency (MIGA) have established early, participatory and ongoing risk assessments as an integral part of their case-related activities.

The IP produces a risk assessment as soon as the complainants make first contact, based on media reports as well as information provided by requesters, CSOs, Country Office staff and the World Bank's Security Office. This assessment is regularly reviewed and updated at each stage of a complaint management by consulting the requesters and their representatives. The risks are assessed in the context of their likelihood and severity.

CAO continues to produce a risk assessment after receiving a complaint and throughout its overall treatment. This is done through constant interaction with the parties as well as consulting with

4 - Frontline Defenders: Workbook on Security: Practical Steps for Human Rights Defenders at Risk (2016), pg. 9

independent sources and IFC/MIGA management. The attention is centred on identifying risk factors and formulating the respective preventive measures.

Several of the human rights mechanisms of the United Nations and CSOs specialized in the protection of human rights defenders also rely on risk assessments to measure the level of risk of reprisals prior to conducting country visits. By way of illustration, the UN Sub-Committee on Prevention of Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment adopted, in 2016, its own set of guidelines on how to prevent and address reprisals. These Guidelines require the Sub-Committee to, in a systematic manner, assess the level and risk of reprisals in the country to be visited. Similarly, the UN Human Rights Office and its field presences conduct regular risk assessments to mitigate the risks of reprisals against individuals with whom it interacts or with whom it has contractual relationships.

NGOs specialized in the protection of individuals and groups at risk, such as Front-Line Defenders, Tactical Technology Collective and Protection International also systematically conduct risk assessments to mitigate risks of harm.

Considerations for conducting a reprisals risk assessment

Based on the practice of international human rights mechanisms and resource organizations employing reprisals risks assessments, it is recommended that the IAMs:

- Integrate the reprisals risk assessment exercise as a key task in all staff work plans.
- Conduct risk assessments for all requests that are brought to their attention, with the view to determine whether and how to proceed with the case.
- Adopt a broad approach to possible victims of reprisals and ensure that the risk assessment addresses risks not only to the persons directly concerned by the case, but also to those associated with them (such as family members) and at risk of reprisal because of this affiliation. For example, the entire family of a requester may have been receiving threats regarding the IAM request.
- Ensure that the risk assessment exercise is participatory – that is, done with the full participation of the persons concerned and, as relevant, CSOs or other third parties that facilitated the complaint to the IAM.
- Consider the expertise of CSOs working with individuals and groups at risk. For example, in high-risk cases, IAMs may wish to compose a risk assessment team with both internal staff and external experts.
- Reach agreement with the person(s) concerned on the measures needed to reduce risks and the actions that could be taken to respond to possible reprisals, should these occur. In developing and implementing these measures, as appropriate, IAMs could work with external actors with expertise in the protection of individuals and groups at risk.
- Regularly review the risk assessments and the measures agreed to reduce risks and respond to reprisals, given that risks depend on the political and security environments in the country and project area, as well as on the stage of the IAM process.
- Conduct separate risk assessments for potential national consultants or service providers who may be at risk because of their affiliation with the IAMs.
- Assess and address risks associated with outreach events through an appropriate risk assessment process.

SUGGESTED TOOLS

TOOL 1: Determine what the assessment should map – deepen understanding the forms of reprisals that may take place in the IAM context.

Risks of reprisals will be unique for each IAM case. However, based on the risks that have been commonly observed in the IAM context, reprisals are often of a similar nature. The risk assessment suggested in this toolkit should seek to establish what form of reprisal may unfold before, during or after the possible IAM intervention in each case, and the capacity of the individuals concerned, on their own, to prevent and respond to the reprisals that have been identified as possible, should these occur.

Common reprisals that the risk assessment could seek to map include, but are not limited to:

- Intimidation, including by indirect and direct threats and verbal harassment against requesters, complainants or others associated with them
- Smear campaigns, including by State-owned media and social media
- Revoking professional permits for individuals (lawyers, trade unions, etc.) and CSOs that support or facilitate the IAM intervention
- Dismissal from employment, or discrimination, disadvantage or other adverse treatment in relation to employment
- Judicial harassment, including retaliatory lawsuits intended to censor, intimidate, and silence critics by burdening them with the cost of a legal defense until they abandon their criticism or opposition (commonly referred to as strategic lawsuits against public participation, SLAPPs) and arbitrary detention
- Physical assault against persons or their property, including their offices and vehicles
- Surveillance by State and non-State actors, including through digital interference.

TOOL 2: Components of a reprisals risk assessment

For the purposes of this toolkit, the level of risk – defined as the possibility that the IAM interaction with the person(s) concerned will result in reprisals – can be established by considering the five components in Box 1:

Box 1. The Five Components of a Reprisals Risk Assessment

1. Understanding the country context: the broader environment for public participation, possible protection concerns and previous instances of reprisals.

2. Understanding key actors and their interests in relation to the project.

3. Assessing whether the confidentiality of requesters, and associated persons, is likely to be maintained throughout the IAM process.

4. Understanding the vulnerabilities and capacities of the person(s) concerned to address the risks and respond to the reprisals that have been identified as possible.

5. Identifying key actors that can support risk-reducing measures and provide important protection channels if reprisals occur.

1. Understanding the country context: the broader environment for public participation, possible protection concerns and previous instances of reprisals.

- As a starting point, a reprisals risk assessment should consider the environment for public participation in the country concerned and seek to understand the extent to which State authorities and other relevant entities demonstrate, in law and in practice, the capacity and commitment to protect individuals and groups against reprisals.[5]

5 - Frontline Defenders: Workbook on Security, 2016. Practical Steps for Human Rights Defenders at Risk, pg. 9.

This layer of the assessment will consider the state of civil society, the situation of human rights defenders, instances of previous reprisals and State authorities' responses to earlier instances of reprisals. The assessment should also identify the main stakeholders to the project at hand, their interests in the project and the possible impacts of an IAM intervention. This assessment may already have been performed by the institution as part of its country and project due diligence.

2. Understanding the key actors and their interests in relation to the project

- When requesters, complainants, and associated persons cooperate with the IAMs, they can challenge the interests of various actors, including those with relative power and authority that have a vested interest in the success of the project at hand and others – including other individuals and communities. The more effective the IAM process is perceived to be in challenging these interests, the greater the risk of reprisal. The key actor analysis should therefore seek to identify these interests and, accordingly, the possible sources of reprisal.

- Understanding the possible sources of reprisals will help the IAMs identify the forms of reprisal that are likely to occur in a case. Equally important, mapping the possible sources of reprisal is key to identifying how, and by whom, these sources might best be influenced if risks are present or if reprisals occur.

- While mapping the key actors requires consideration of the project under review and its geographic location, it could also consider the findings of the general risk context assessment (Component 1). For example, IAMs could determine if regions or towns involved in the project and its area of influence are mentioned in human rights reports, if there are agencies or persons noted as problematic, and if other development lending institutions or companies in the area are experiencing problems.[6]

3. Assessing whether the confidentiality of requesters and associated persons is likely to be maintained throughout the IAM process.

- Maintaining confidentiality can be one of the most effective ways to reduce risks of reprisals. It is therefore important for the IAMs to assess whether the confidentiality of persons concerned can realistically be maintained throughout the process. For example, a group of requesters may already have had to voice their concerns or make known their intention to submit a request to an IAM due to specific requirements of the process. This could generate an increased risk of reprisals.

- To assess possible risks related to protecting the identity and identifying information of the requesters, IAMs need to seek, from the person(s) concerned, information about entities and individuals to whom they have talked about the case and the issues raised in the complaint, and determine whether the requesters are likely to be identified when it becomes known that a request has been received by the IAM.

4. Understanding the vulnerabilities and capacities of the person(s) concerned to address the risks and respond to the reprisals that have been identified as possible.

- Based on the (forms of) reprisals that have been identified as possible, IAMs are advised to consider the vulnerabilities and capacities of the person(s) concerned to address these risks on their own, and to respond to the reprisals by themselves should these occur. In simple terms, a person's vulnerabilities and capacities should be assessed in relation to each possible reprisal. For example, if legal harassment by State authorities is considered likely and the requester has very limited understanding of the national legal framework and no access to legal support, he or she will be at high risk of harm in relation to that risk.

- It is important to note that each risk assessment

6 - Taylor, Zandvliet, and Forouhar, 2009. Due Diligence for Human Rights: A Risk-Based Approach (Corporate Social Responsibility Initiative Working Paper No. 53), pg. 10.

will be different in terms of assessing vulnerabilities and capacities, as these will vary greatly according to the persons at risk and to the unique context of the case (see Box 2)

Box 2. Definitions of "Vulnerability" and "Capacities" of Persons at Risk

Vulnerability is defined as the degree to which the person(s) at risk (requesters, complainants and other cooperating persons, depending on scope of the assessment) are susceptible to loss, damage, suffering, and, in a worst-case scenario, to death in the event of a reprisal.

Capacities are the strengths and resources that the individual(s) can access to achieve a reasonable degree of security (such as abilities or contacts).

Source: *New Protection Manual for Human Rights Defenders* (Protection International), by Enrique Eguren and Marie Caraj, 2009.

- The vulnerabilities and capacities of the individual(s) concerned determine the extent to which they themselves can reduce the likelihood that a reprisal will occur and how effectively they can respond to instances of reprisals that occur.

- In any given situation, anyone seeking to access an IAM may face a common level of risk of reprisal. But not everyone is equally vulnerable to that risk.[7] Vulnerability varies according to several factors, as the examples that follow illustrate:

  - There may be a country where the Government poses a general threat to human rights work. In this context, everyone the IAMs interact with in the country could be at risk of reprisal for that interaction. But some individuals or groups could be more at risk than others. For example, a large well-established CSO based in the capital may not be as vulnerable as a small, local CSO.[8]

  - Different people face different risks, and it is important to consider which of their personal attributes may make them more vulnerable to risks of reprisal. In most societies, for instance, female requesters face additional risks because of who they are and how they express themselves.[9] In other cases, indigenous communities with limited literacy in the national language may be more vulnerable to attacks due to their inability to communicate in the language shared by the other stakeholders to the IAM process.

  - Vulnerability can also include lack of safe ground transportation, lack of access to a phone or to other means of communication, limited awareness about the risks of surveillance when using communication tools, or lack of connections to international CSOs or other actors that could provide important protection if reprisals occur.[10]

  - Vulnerability may also relate to fear. For someone who has received threats and has no proper way of dealing with this fear (such as good networks to activate a response to the threats), chances of making mistakes or poor decisions that can create further risk of reprisal are higher.[11]

  - Capacities and vulnerabilities are often two sides of the same coin.[12] Some other examples

7 - See Eguren and Caraj, 2009. New Protection Manual for Human Rights Defenders (Protection International) for a discussion on vulnerability and capacities.

8 - Ibid., pg. 28. Aggressions against requesters, complainants and others associated with them in rural areas may be less public and therefore provoke less reaction at law enforcement level and political level than aggressions in urban areas. Stakes are higher for attacks against CSO headquarters or high-profile organization s in urban areas, as these would generate a greater reaction (Ibid., pg. 56).

9 - Frontline Defenders, 2016. Workbook on Security: Practical Steps for Human Rights Defenders at Risk, pg.3.

10 - Eguren and Caraj, 2009. New Protection Manual for Human Rights Defenders (Protection International), pg. 29.

11 - Ibid.

12 - Ibid.

of important capacities – or vulnerabilities, if the person(s) concerned do not have these capacities – in the IAM context are:

- A good understanding of the relevant operational safeguards that have been, or will be, invoked in the request for problem-solving or compliance review (to the extent these support rights the individual or group would have under parent institution policies).
- Good relations with other community members and neighboring communities, and support from these to bring the case to the IAM(s).
- Access to communication equipment, such as telephones and computers, and an understanding of how to reduce risks of surveillance.
- Access to safe ground transportation.

5. Identifying key actors that can support risk-reducing measures and provide important protection channels if reprisals occur

• Because IAMs are limited in what they can do to mitigate risks and respond to reprisals, identifying external alliances is essential. A final level of the risk assessment therefore identifies the actors that can improve the security of requesters or other related stakeholders by providing support for measures to reduce risks and/or responding to reprisals if these occur.[13] Examples include CSOs with significant experience working with individuals or groups at risk of reprisal or a UN Human Rights field presence that could activate protection mechanisms if risks of reprisal are imminent.

- A list of suggested resource organizations is provided in the appendixes.

TOOL 3: Guiding questions for the risk assessment

For ease of reference, guiding questions for each of the five components of the risk assessment and hyperlinked sources of information are suggested in Table 1.

IAMs are encouraged to consider all suggested sources rather than relying on only one for the risk assessment exercise. Suggested sources may not necessarily cover all regions or all issues, may change over time, and should be viewed in a complementary fashion to address the specific issues of a case.

Table 1. Guiding questions for the risk assessment

Component 1. The broader environment (national level)

Topic	Suggested questions	Sources of information
Environment for public participation	•What does the record of human rights in the country say about existing abuses in general? •Who are the most likely perpetrators of abuse? •Is there impunity? •Are there patterns of discrimination against certain groups? •What is the state of civil society? Are there current or draft laws that reduce the rights of CSOs to pursue their work? •What is the situation for human rights defenders? Have precautionary measures been issued for individuals or groups in the country? •Is there capacity and commitment of the national authorities to respond to protection concerns?	The requesters and other related stakeholders Other potential sources (see Appendix 1 for links): •Amnesty International's country profiles •CIVICUS Civic Space Monitor •Commissioner for Human Rights of the Council of Europe •Concluding observations of the UN CERD Committee •Concluding observations of the UN Human Rights Committee •Frontline Defenders

13 - For example: national witness protection programs or specific protection programs for human rights defenders; international or regional intergovernmental organization(s) (with presence in the country or region) with a mandate to monitor and/or protect human rights; international CSOs (with presence in the country or region) with expertise in the protection of human rights defenders.

	•Are there laws or mechanisms to protect human rights defenders, and what is their effectiveness and integrity?	•Human Rights Watch country reporting •International Service for Human Rights, which has produced a Reprisals Handbook (ISHR) •Precautionary measures of the Inter-American Commission •Protection International •Reports of the UN Human Rights Office's field presences •The Special Rapporteur on human rights defenders of the African Commission •The Special Rapporteur on human rights defenders the Inter-American Commission •The UN Special Rapporteur on human rights defenders •UN and NGO compilation reports or the Universal Periodic Review
Previous instances of reprisals and responses to protection concerns	•What are the past actions of the Government (and possible opposition groups) with regard to persons who have testified about sensitive topics? Have there been attempts to silence witnesses and informants in the past? •What forms have these reprisals taken? •Are there specific points in time where reprisals have been more frequent?	External sources of information

Component 2 . The key actors (project level)

Topic	Suggested questions	Sources of information
Key actors (possible sources of reprisal)	•Is there a history of reprisals against the person(s) concerned? Who has retaliated and what forms have the reprisals taken? •Do the parties to the IAM process have a record record of retaliating? •How might the IAM process negatively affect the interests of actors that have an interest in the success of the project? •Are they aware of the requesters' concerns about the project and their intent to submit a complaint to the IAM? •Who/what group(s) are the possible sources of retaliation? •What does their power and readiness appear to be to do so? • What forms of reprisal are these sources likely to employ?	The requesters and other related stakeholders Other IAMs Internal country and project-related reports of the IAM's parent institution Reports of CSOs active in the project area Other sources (see Appendix 1 for links): •Annual reprisals-reports of the UN •Secretary General •Front Line Defenders •ISHR •Protectdefenders.eu •The Special Rapporteur on human rights defenders of the African Commission

	•What is the political cost of retaliating? What are the chances of them getting away with reprisal undetected? •How can the possible sources of reprisal best be influenced to reduce risks?	•The Special Rapporteur on human defenders the Inter-American Commission •The UN Special Rapporteur on human rights defenders

Component 3. Confidentiality (individual level)

Topic	Suggested questions	Sources of information
Risks to maintaining confidentiality	•Have the requester(s) or complainant(s) reported the issue before, or said they would do so? • Can the issues identified be readily attributed to the requesters(s) or complainant(s) or others supporting their case? •Can the case proceed without identifying the persons concerned? •What is the risk that the subject of the request will guess/ascertain who made the request?	Discussions with requesters to assess to what extent they have already raised their concerns with the parent institution clients or subclients and/or publicly.

Component 4. Vulnerabilities and capabilities (individual level)

Topic	Suggested questions	Sources of information
Vulnerabilities and capacities of person(s) to address risks and respond to threats identified	Bearing in mind that IAMs should always assess the level of vulnerabilities and capacities in relation to each identified risk, these are illustrative examples only and should be tailored to the unique circumstances of each case. •Does the person(s) concerned live in remote or isolated areas? •Does the person(s) belong to a group that is disadvantaged or discriminated against? •Does the person(s) work on sensitive issues (before, or in parallel, to the IAM process) that could put them at higher risk of reprisal? •Does the person(s) have good knowledge about their rights under national laws and policies? •Does the person(s) have good understanding of their rights under the operational safeguards and other policies that have been invoked in the request to the IAM? •Does the person(s) concerned have sufficient mediation skills? •Does the person(s) have good knowledge of how to deal with stress in the face of possible threats and reprisal? •Does the person(s) enjoy the support of their own community and neighboring communities to bring the case to the IAM?	Assessing vulnerability and capacities is largely subjective and will be based on the feedback of those concerned (requesters and other cooperating persons)

	•Does the person(s) have good networks that can be accessed for protection strategies (e.g. legal assistance) and how resourceful are these networks? •Does the person(s) have access to influential actors and people for support to their cause (e.g. powerful allies within the State administration or police, international and regional human rights mechanisms, or embassies that can provide support for human rights defenders at risk)? •Have the person(s) adopted plans and measures to address risks to security (e.g. contingency plans for foreseen risks and emergency plans for unexpected risks)? •Does the person(s) have a good public reputation? •Does the person(s) have access to relevant physical and IT (information technology) security, including secure offices/ communication means and an understanding of how those could be intercepted if no precautionary measures have been taken? •Does the person(s) have access to safe housing, safe ground transport and financial resources?	

Component 5. Sources of protection (international, national and project level)

Topic	Suggested questions	Sources of information
Key actors (possible sources of protection)	•Who are the key actors that can provide support for measures to reduce risks, and address reprisals, including through protection, should these occur?	National witness protection programs or mechanisms dedicated to the protection of human rights defenders. Potential protection resources at the community level, such as local protection networks. Other sources (see Appendix 1 for links): •EU Diplomatic Missions •Front Line Defenders •National witness protection programs or mechanisms dedicated to the protection of human rights defenders •Peace Brigades International •Potential protection resources at the community level, such as local protection the community level, such as networks •Protection International •UN Human Rights Office field presences

ACTION 2: CONDUCT A LEANER PRELIMINARY RISK ASSESSMENT AS PART OF THE ELIGIBILITY ANALYSIS

What it is

IAMs may wish to consider conducting early reprisals risk assessments as part of the initial analysis they systematically undertake to determine the eligibility of incoming requests.

Why it is important

Conducting a risk assessment at the eligibility stage is important because if it indicates that an IAM intervention could have serious repercussions for the safety of those concerned, the mechanism will need to decide whether to postpone or fast-track the registration of the case, or whether to proceed with it at all.

SUGGESTED TOOLS

TOOL 1: Risk assessment template
Assessing risk for requests can be done through a leaner risk assessment that considers, at a minimum, Components 1, 2, and 3 (See Box 1).

Guidance on questions to be applied and sources of information can be found in Table 1.

Risk assessment template
Case name/number
Assessment date
Name of officer responsible for assessment
Component 1. The broader environment for public participation, previous instances of reprisals and Government responses to these
Component 2. The key actors with a vested interest in the success of the project, and previous instances of threats and other forms of reprisals against the person(s) concerned
Component 3. Whether confidentiality can realistically be maintained throughout the IAM process.

ACTION 3: ASSESS AND ADDRESS RISKS FOR LOCAL CONSULTANTS AND SERVICE PROVIDERS

What it is

IAMs may wish to consider conducting separate risk assessments for local consultants as part of the recruitment process to assess the likelihood of consultants facing reprisals because of their involvement in the IAM intervention.

Why it is important

Reprisals against local consultants and service providers (interpreters, drivers, and others facilitating the IAM intervention in the country concerned) have been observed in the IAM context. Considering that site visits, dispute resolutions processes, and investigations undertaken by IAMs generally require hiring of local consultants and/or service providers, IAMs must be able to assess whether their collaboration with IAMs might lead to them facing reprisals and seek to avoid or mitigate this risk. Risks of reprisal to local consultants and service providers often correlate to the degree of insecurity and instability of the country or the region[14] of the given IAM case, and entities promoting the development activity may perceive that the IAM intervention threatens or interferes with sovereign affairs of the country.[15]

Reducing risks to local consultants or service providers

If the reprisals risk assessment for local hires indicates a high probability of reprisals, measures can be taken to mitigate risks. These measures include rotating local hires when interacting with the authorities, and not disclosing personal or contact details.

When risks cannot be mitigated, IAMs may wish to favor the hiring of other service providers who are at lesser risk.[16]

Example

The organization Red T, in partnership with the International Association of Conference Interpreters and the International Federation of Translators, has developed a Conflict Zone Field Guide for Civilian Translators/Interpreters and Users of their Services. This guide outlines the basic rights, responsibilities and practices recommended by the three organizations. It applies to translators/interpreters as field linguists for the armed forces, journalists, CSOs and other organizations working in high-risk settings. The guide is available at http://red-t.org/guidelines.html.

14 - Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, pg. 22.

15 - Ibid.

16 - Ibid.

SUGGESTED TOOLS

TOOL 1: Suggested risk assessment template for local hires

A risk assessment for local hires could focus on the broader environment for public participation, previous instances of reprisals and Government responses to these (see Box 1, Component 1).

Risk Assessment Template for Local Hires	
Case name	
Assessment date	
Name of officer responsible for risk assessment	
Component 1. The broader environment for public participation, previous instances of reprisals and Government responses to these	
Does the local hire have any links to the project under review? (e.g. family members living in the area)	
Does the local hire have any links to the IAM's parent institution? (e.g. the interpreter or driver has previously worked for the IAMs' parent institution in the country)	
Has the local hire, before or in parallel with the IAM process, pursued human rights advocacy or engaged with international or national CSOs and may, because of this engagement, be subject to reprisals by national authorities or other non-State actors in the country?	

ACTION 4: UNDERSTAND RISKS RELATED TO IAM OUTREACH EVENTS

What it is

Organizing outreach events involving participants who are already the subject of reprisals (for example, due to previous activism) or in locations in which participant involvement in the outreach event might lead to reprisals, requires IAMs to assess risk through a stand-alone assessment and take measures to reduce risks when relevant.

Why it is important

Threats and other forms of reprisal have been observed against participants to IAM outreach events, particularly in countries where freedom of association or speech are restricted. Understanding these risks is key to making informed decisions about whether the event should be held, and the kind of measures needed to reduce possible risks.

SUGGESTED TOOLS

TOOL 1: Suggested risk assessment template

An assessment of risks to participants and facilitators could, at a minimum, consider:

- The general country context reported reprisals and Government responses to reprisals (See Box 1, Component 1)
- The current state of play for civil society, and whether there are current or draft laws that seek to restrict freedom of expression and opinion or otherwise complicate registration and work of civil society organizations (See Box 1, Component 1)
- Whether there are sensitivities on the part of the State regarding current or planned development projects in the country, including, but not limited to, projects funded by the IAMs' parent institutions
- Whether there are possible tensions between the possible participants that could jeopardize their security
- Whether participants are at risk for participating in the event or for being associated with the organizers of the event.

TOOL 2: Further guidance on security considerations when organizing outreach events

An assessment of risks related to outreach events could benefit from the expertise of relevant civil society organizations, particularly organizations working locally. Such organizations are often well placed to advise IAMs on appropriate measures to reduce risks and respond to possible reprisals.

IAMs may wish to contact resource organizations with expertise in the protection of individuals and groups at risk, such as Front-Line Defenders, Protection International or the UN Human Rights Office, to solicit more information about country-based CSOs that could support IAM risk assessments for outreach events and/or plan and implement security measures to reduce risks.

Materials that might help IAMs develop their own risk management strategies include. "Creating a Safe Space," in Holistic Security - Trainer's Manual) (Tactical Technology Collective), 2016, pgs. 8–9).

https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/60/holisticsecurity_trainersmanual.pdf

PHOTO: MICI

DEVELOPING STRATEGIES TO REDUCE IDENTIFIED RISKS

Individuals at risk of reprisals are often unable, in part or fully, to reduce risks of reprisals that relate to their interaction with the IAMs. In this regard, the IAMs play an important role to help those at risk plan and implement appropriate risk-reducing strategies. Once IAMs have mapped the risks of reprisals that relate to a case, an important follow-up action is to identify and implement, with the people concerned, appropriate measures that can reduce the level of risk.

Expert organizations working to protect individuals and groups at risk emphasize that a risk assessment should result in the design of appropriate measures to reduce the identified risks to an acceptable level. Similarly, the reprisals guidelines issued by the World Bank Group's Inspection Panel[17] and the Compliance Advisor Ombudsman[18] highlight the responsibility of the mechanisms to plan and implement measures to reduce risks and note the important role that external resource organizations can play in designing and supporting these kinds of measures.

Risk-reducing strategies can take several forms. Selecting one does not exclude the possibility of implementing others. The following six actions may serve to guide the process:

- Design and implement specific measures to build reduce vulnerabilities and increase capacities of those at risk.
- Address power imbalances.
- Choose discretion or visibility as a protection strategy.
- Clarify to all parties that reprisals will be dealt with seriously and addressed throughout the IAM process.
- Manage expectations of requesters and complainants.
- Choose whether, when, and how to proceed with a case.

ACTION 5: DESIGN AND IMPLEMENT MEASURES TO REDUCE VULNERABILITIES AND INCREASE CAPACITIES OF THOSE AT RISK

What it is

Where immediate risks have been reduced or are less present, IAMs are advised to reach a common understanding with the relevant person(s) on practical measures the IAMs can reasonably take – whether by their own actions or by referring those at risk to other support mechanisms – to reduce the vulnerabilities and capacities of those concerned to address the risks that have been identified. Any such agreement should be tailored specifically to reducing vulnerabilities and supporting capacities of requesters to proceed with their complaints with reduced risk of reprisals and avoid reflecting a bias in favor of the complainant.

17 - Inspection Panel, Guidelines to Reduce Retaliation Risks and Respond to Retaliation During the Panel Process. http://inspectionpanel.org/sites/ip-ms8.extcc.com/files/documents/IPN%20Retaliation%20Guidelines_2018.pdf

18 - Compliance Advisor Ombudsman, CAO Approach to Responding to Concerns of Threats and Incidents of Reprisals in CAO Operations, http://www.cao-ombudsman.org/documents/CAO-Reprisals-web.pdf

Why it is important

Requesters and other related stakeholders rarely have the capacity on their own to reduce risks of reprisals and to respond to reprisals that may occur. As such, they are dependent on the IAMs and/or other resource organizations to help them mitigate these risks.

To lessen the possibility that someone will inflict harm through purposeful retaliatory action, any risk-reducing strategy should systematically pursue a two-pronged approach:

- Reduce the vulnerabilities of the person(s) at risk, enabling them to respond to possible reprisals in an effective manner and mitigate the identified risk.

- Increase the capacities of the person(s) at risk to reduce and respond to possible reprisals in an effective manner (thereby reducing vulnerabilities).[19]

Example

Resource organizations with expertise in protecting individuals and groups at risk, such as Front-Line Defenders and Protection International, reduce vulnerabilities to risk by increasing the capacities of those at risk to be able to respond to threats in a more systematic manner.

SUGGESTED TOOLS

TOOL 1: Map needs in relation to existing vulnerabilities

Risks that have been identified in the risk assessment exercise should give the IAMs a good indication of measures that are needed and which party/parties, if not the IAMs, is/are well placed to provide support.

IAMs may not be able to advise requesters and other stakeholders on how to enhance their physical or digital security or strengthen their knowledge of the national laws that have (or should have been) applied to the project under review.

Table 2 illustrates how to develop a strategy for strengthening existing capacities and reducing vulnerabilities. It should be noted, however, that when risks of high-impact reprisals are imminent (such as physical attacks that can lead to significant bodily harm), it is not safe to try to reduce risk by increasing capacities, given that capacity building takes time.[20]

In these situations, IAMs should focus their efforts on discussing with at-risk persons how threats can best be reduced, i.e., discuss whether IAMs can directly influence the source of the threat or engage with other entities that can exercise positive influence over the situation, including management of the IAMs' parent institutions, the UN Human Rights Office, or other mechanisms with a protection mandate.[21]

19 - This formula is based on Eguren and Caraj, 2009. New Protection Manual for Human Rights Defenders (Protection In ternational), pg. 30.

20 - Ibid, pg. 31.

21 - Front Line Defenders, Protection International, or Tactical Technology Collective might provide additional guidance. See Appendix 1.

Table 2. How to develop a strategy to strengthen capacities and reduce vulnerabilities of persons at risk of reprisals

Identified risks and source of reprisal	Existing vulnerabilities of person(s) at risk	Existing capacities of person(s) at risk	IAM actions to strengthen capacities and/or reduce vulnerabilities
Stigmatization and smear campaign	No support for the IAM intervention by other community members and influential actors in the area. Smear campaign will aggravate this.	None	Issue public statements in support of the requesters' right to access the IAM (without prejudice to the outcome of the case). Ask parent institution or other relevant institution(s) to issue a statement of this kind. Contact parent institution(s) for them to engage with borrower/ fund recipient/client/subclient.
Risk of demotion or termination of employment	No support from senior leadership of company or trade union.	None	Engage with parent institution(s) to raise awareness of the risk and seek their support in communicating the concerns to the borrower/fund recipient/ client/subclient. Communicate zero tolerance of reprisals of this kind at the earliest stages of the process to mobilize support.
	Limited awareness on the part of requesters and other workers about rights under relevant parent institution safeguards.	Initial contact has been established with CSO active in the country with significant knowledge about labor rights, including under relevant parent institution safeguards.	Share relevant parent institution policies and procedures. Encourage engagement with relevant CSOs.
Arbitrary detention	No contacts to organizations that could provide legal and other assistance.	None	Refer requesters to appropriate CSOs that can provide legal support.
Interception of sensitive communication to the IAMs and other contacts	None	A CSO in the area has previously worked with the requesters to establish safe lines of communication.	Seek to establish jointly agreed alternatives for safe exchange of information.

ACTION 6: ADDRESS POWER IMBALANCES

What it is

In a given case, IAMs may wish to consider how to best address power imbalances between requesters and entities that may seek to retaliate.

Why it is important

The IAM processes may take place in a context in which requesters and/or complainants feel intimidated and unable to address their fears of reprisal. Such an unsupportive environment often relates to power imbalances between the parties to the IAM process: complainants are rarely equal in power to, for example, the project implementing agency (in the case of problem solving) and to management of the IAMs' parent institutions (in the case of compliance reviews) and other entities. This asymmetry leads to a dilemma because if one side is stronger, the outcome may favor that party.[22] It also means that the weaker party – the requester and/or complainant – is susceptible to reprisals, including intimidation and other forms of harassment meant to make them cede their case.

Examples

CAO, in its Approach to Responding to Concerns of Threats and Incidents of Reprisals in CAO Operations, commits to working with the parties to its process to implement measures that address power imbalances. Such measures include the engagement of professional mediators, and provision of training, and ongoing capacity building for the parties engaged in dialogue.

Several other IAMs are also taking important measures to level the playing field, in particular in the context of problem solving. These measures are illustrated in the tools section.

SUGGESTED TOOLS

TOOL 1: Suggested measures to "level the playing field"

Several of the IAMs are already taking important measures to level the playing field in the context of problem solving. Such measures include:

• **Agreeing on ground rules for sharing information.** Ensuring that all parties have the same access to the same information at the same stage of the process, in a format that is accessible to them (for example, if the requesters are a Creole-speaking community in Haiti, in Creole rather than French).

• **Ensuring that meeting places and times are logistically feasible for complainants.** For instance, it may be expensive for complainants to meet in a municipality far away from where they live. In this case, IAMs have provided safe ground transportation to facilitate the complainants' access to the meeting venues.

• **Building the capacity of complainants and persons associated with them to better understand their rights under relevant safeguards and negotiate the practical terms for those rights in the IAM process.**

Capacity building is a particularly important measure to reduce the vulnerability of complainants to reprisals. Capacity building should seek to enhance complainants' understanding of their rights under relevant social and environmental safeguards, and to develop negotiation and other skills typically needed for supporting their complaint. While external resource organizations may be better placed than the IAMs to provide such training, IAMs are encouraged to ensure that these kinds of measures are considered an integral part of the problem-solving or compliance review processes and are supported financially.

22 - United Nations Institute for Training and Research, Department of Political Affairs, 2010. A manual for UN mediators – Advice from UN Representatives and Envoys, pgs. 33–35.

ACTION 7: CHOOSE DISCRETION OR VISIBILITY AS A PROTECTION STRATEGY

What it is

IAMs' interactions with requesters, complainants, and related associates can be either visible or discreet. While discretion is often used as the standard approach, it may not always be the best way to prevent reprisals. In some situations, IAMs can discourage perpetrators from retaliating merely through their presence and the visual impact of their involvement.

IAMs may therefore wish to assess, on a case-by-case basis, if discretion or visibility will give requesters, complainants, and others the best protection against reprisals.

Why it is important

The decision to retaliate is never made in a vacuum – every decision is affected by a series of calculations and perceptions, whether by a single individual or by many actors in a complicated chain of command.[23] Through presence and visibility, an IAM can influence these decisions by creating circumstances in which the perpetrators recalculate the consequences and make different choices.[24] Put differently, in a given situation, if the IAMs' interaction with the requesters is not made public, the cost of retaliating is low.[25] If the IAM (or other actors of the international community) makes its/their presence known, the cost could be higher, helping to lower the probability of reprisals.[26]

SUGGESTED TOOLS

TOOL 1: Determine whether discretion or visibility is the best strategy

Requesters often have the best understanding of their own risk context. To determine whether visibility would be a viable approach to reduce risks of reprisals, IAMs could consider proactively discussing these options with requesters, complainants, and their associates.

However, the use of visibility strategies should be assessed case by case to avoid situations for which increased visibility could be counterproductive. For example, as has been noted by the UN Office of the High Commissioner for Human Rights, increased visibility might be counterproductive when the IAM is widely perceived as a "foreign interferer" either nationally or locally.[27]

TOOL 2: Use visibility as a protection strategy

Choosing visibility implies that IAMs proactively make their presence known. If visibility is considered the best option, IAMs should agree with those concerned on measures that should be taken as part of this strategy.

IAMs can increase their visibility in several ways, including by:

- Making use of an official vehicle of the parent institution when parking outside an individual's house or organization's house, to publicize the IAM's presence.
- Issuing press releases before, during, or after the principal field visit (or all three times), or upon the conclusion of the IAM process.
- Working with other international or national actors who, through their visible presence, can offer additional protection. Such actors can include diplomatic representatives, high-profile human rights personalities, UN field presences (specifically, the local UN Human Rights Office), and national human rights institutions.

23 - Mahoney, 2006. Proactive Presence: Field Strategies for Civilian Protection (Centre for Humanitarian Dialogue), pg. 16.

24 - Ibid.

25 - Ibid.

26 - Note, however, that perpetrators' notions of 'acceptable' consequences can be fluid over time and will vary greatly among individuals and organizations. Usually, perpetrators have interests and motivations for being sensitive to international presence. Effective international presence plays on all of these interests and motivations, reducing the amount of abusive actions that remain acceptable to the abuser (Ibid., pgs. 16–17).

27 - UN Office of the High Commissioner for Human Rights. Manual on Human Rights Monitoring Chapter 30: Using Presence and Visibility, pg. 4.

ACTION 8: CLARIFY TO ALL PARTIES THAT REPRISALS WILL BE CONSIDERED AND ADDRESSED THROUGHOUT THE IAM PROCESS

What it is

An important strategy to reduce risks of reprisals throughout the IAM process is to ensure that the public and all parties involved in the project – including borrowers and other recipients and/or clients, project implementing agencies, and parent institution management – are clearly informed that any form of reprisal is unacceptable and that reprisals, should they occur, will be addressed.

Why it is important

Publicizing the fact that reprisals will be monitored and addressed serves two important purposes. First, it creates greater challenges for retaliatory acts, as possible perpetrators are made aware that reprisals will not be tolerated. Second, it encourages requesters and complainants to report reprisals, making a rapid response by the IAM and others possible.

Examples

The standard practice of UN Human Rights Mechanisms is to explain from the outset that no reprisals should take place and that these will be addressed, should they occur. By way of illustration, the UN human rights treaty bodies have included making the protection of members of civil society and others a regular item on the agenda of informal meetings with States parties, and broadly disseminate their guidelines on reprisals.

Similarly, in its guidance on Commissions of Inquiry and Fact-finding Missions, the UN Human Rights Office recommends that standard language on reprisals be included in early public statements. This is particularly important if the Commissions or Missions do not have an explicit reference to the protection of all persons cooperating with them in their mandates and/or terms of reference.

SUGGESTED TOOLS

TOOL 1: Share IAM policy on reprisals with all parties to the process

The IAMs that have already developed a policy on reprisals may wish to consider disseminating it to all parties in a given case, at the earliest stages of the process.

In keeping with the practice of the UN Human Rights Treaty Bodies, IAMs can also consider including reprisals as a standard discussion item for both problem solving and compliance review to ensure that all instances of reprisals are reported and addressed.

TOOL 2: Include general reference to reprisals in public registration notices

Including a general reference in public registration and other case-related documents could help enhance acceptance among all parties to the IAM processes – including implementing agencies and management of the parent institutions – that risks of reprisal will be continuously addressed throughout IAM operations.

ACTION 9: MANAGE EXPECTATIONS TO REDUCE RISK-TAKING BEHAVIOR

What it is

Requesters and other related stakeholders sometimes erroneously believe IAMs have relatively significant power to prevent reprisals, including, for example, through halting execution of a project if reprisal threats are posed. In these situations, requesters and complainants take higher than necessary risks to approach the IAMs.

Why it is important

Requesters to IAMs are often vulnerable to reprisals because they have a limited understanding of what the IAMs can and cannot do to remedy grievances and provide protection against reprisals.

When requesters do not understand the limited influence IAMs have over the situation, they may be taking high risks when requesting IAM intervention (for example, being open and vocal to the project implementing agency or other community members about going to the IAM). Requesters also take additional risks if they believe IAMs can somehow protect them against reprisals.

It is, therefore, important for IAMs to manage expectations from the beginning, and, in this way, prevent requesters and related third parties from adding to the risk of reprisals.

Examples

CAO, in its Approach, emphasizes that it seeks to be clear about the limitations of its ability to respond to instances of threat and reprisal. "CAO is not an enforcement mechanism and does not have any direct ability to physically protect complainants or otherwise safeguard people from possible consequences of engaging in a CAO process or cooperating with CAO." (Approach to Responding to Concerns of Threats and Incidents of Reprisals in CAO Operations)

The UN Office of the High Commissioner on Human Rights, in its guidance on the protection of victims, witnesses, and other cooperating persons, also highlights the importance of providing a clear and accurate explanation on the limitations of the Office to provide protection in the case of threats or other forms of reprisals (Chapter 14 of the Manual on Human Rights Monitoring).

SUGGESTED TOOLS

TOOL 1: Prepare an information sheet or include information in a public statement describing what IAMs can and cannot do to address reprisal risks.

IAMs may wish to consider preparing an information sheet for requesters and supporting organizations, or otherwise clearly inform them from the start, about what requesters can realistically expect in terms of outcome and possible support to respond to reprisals. Alternatively, IAMs developing a public policy on reprisals can include this information in the policy and ensure that the policy is distributed in the context of a request for problem solving or compliance review.

The information sheet could indicate the following:

- The IAM can engage in problem-solving or compliance review processes but cannot always guarantee that senior management of its parent institution will take all actions to address reprisals.
- Approaching the IAM might come with risks of reprisal, the IAM is limited in what it can do to prevent and address reprisals, and requesters and supporting individuals and organizations must actively think about their own safety and put in place measures to reduce risks.
- The IAM can proceed with a compliance review, but the outcome will hinge on a Management Action Plan over which the IAM has often limited control.
- A list should be provided of CSOs and human rights mechanisms that may be able to provide support to reduce risks and address reprisals, should these occur.

ACTION 10: CHOOSE WHETHER, WHEN, AND HOW TO PROCEED WITH A REQUEST OR ONGOING CASE

What it is

Once the IAMs have established the level of risk in a given case, a key step to address risk is to decide whether and when to proceed with a request (or with a case that is already active but with a changed risk context).

If risks of reprisals are present, IAMs are encouraged to decide whether to:

- Proceed with registering the case or to continue its processing (problem-solving or compliance review) if it is underway;

- Postpone intervention until a later stage when risks have been mitigated or are less present; or

- Develop a fast-track intervention to reduce growing risks of reprisal.

Why it is important

In some cases, a reprisals risk assessment may indicate that an IAM intervention poses significant risks to the safety of requesters and others associated with them. In this case, intervening at the wrong time (or intervening at all) can have far-reaching consequences to the persons concerned.

Examples

In the IAM context, former members of the World Bank's Inspection Panel have noted the importance of choosing the timing for IAM intervention carefully. In one occasion, Panel members opted for postponing registration and investigation of the case due to upcoming elections, which it considered would add to the risk of reprisals.

In the context of international human rights hearings, the European Court of Human Rights has noted that "the period between the registration of an application with the Court and its communication to the authorities of the respondent state may be particularly dangerous for applicants in terms of the exercise of pressure' and, as such, has given priority to the scheduling of hearings on cases in which petitioners have faced pressure"

See Vega Gonzales and Ferstman: Ending Threats and Reprisals against Victims of Torture and Related International Crimes (2009), pg. 49.

SUGGESTED TOOLS

TOOL 1: Guidance to assess whether to intervene

According to guidance by the UN Office of the High Commissioner for Human Rights, IAMs are advised to:

- Always consider the views of those concerned in making the final decision about whether to intervene.

- Not proceed with a request or an already registered case if risks of serious reprisals are high and there is no scope to reduce risks to an acceptable level.[28]

- Not proceed if there is not enough information to make an informed decision about the level of risk.[29]

- Always be able to publicly explain the reasoning behind the decision not to intervene.

- Make a public statement about the decision not to intervene if this does not further jeopardize the safety of those concerned.[30]

It should be noted that the decision not to register or proceed with a case does not reduce the IAMs' responsibility to seek to influence the situation, if this does not pose additional security issues to the person(s) concerned. Where risks of high-impact reprisals are imminent (such as physical attacks that can lead to significant bodily harm), the IAMs should always assess whether there is scope for them to reduce risks by engaging with the source of the threat or asking others that can influence the source to do so (such as the IAM's parent institution or a field presence of the UN Office of the High Commissioner for Human Rights). In any case, the requesters should first be informed of the decision and the reasons for it before action is taken.

28 - UN Office of the High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14 Protection of Victims, Witnesses and other Cooperating Persons, pgs. 8-9.

29 - Ibid.

30 - Office of the UN High Commissioner for Human Rights, 2015. Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law, pg. 77.

TOOL 2: **Guidance to determine the ideal timing for an intervention**

When deciding how to proceed with a case, IAMs will need to consider if there are specific moments or periods during which reprisals have been more frequent (for example, before or during elections; after publishing reports or naming key figures publicly; or before, during, or after demonstrations, anniversaries, and/or high-level visits). The risk assessment template presented in the preceding section would, in some degree, cover specific instances when risks appear higher. Such circumstances may warrant postponing IAM interventions (including field visits) to a time when security is less volatile.

In other cases, the risk assessment may conclude that a speedy IAM intervention could minimize risks of reprisals. In this regard, it should be noted that in the IAM context, reprisals have commonly been observed to happen in the period between the receipt of the request and the determination of eligibility. At times, reprisals have diminished in both gravity and frequency when these cases have moved quickly. Where the situation so merits, IAMs should fast-track the registration of cases and the subsequent process (problem solving or compliance review).

Although choosing the best timing for an IAM intervention can be an important way to address risks of reprisal, some IAM procedures do not provide flexibility for doing so. In such cases, IAMs may consider engaging with the boards of their parent institutions to raise awareness and suggest introducing language in upcoming procedural revisions or agree on ad hoc measures through case by case waivers.

PHOTO: TGOLDMAN ENVIRONMENTAL PRIZE

Berta Cáceres,
Honduras.

RESPONDING TO ALLEGED THREATS AND REPRISALS

ACTION 11: DEVELOP AND PURSUE MEASURES ON A PROTECTION TIMELINE

What it is

When IAMs receive information about alleged reprisals, including threats about actual or potential harm, a protection timeline to implement previously discussed and/or new measures could be developed. This should occur in close consultation with the person(s) concerned.

Why it is important

Responses to reprisals should be based on the principle of "do no harm" (that is, do not further jeopardize the safety of the victims or others associated with them). This requires gathering and verifying information related to allegations of reprisal,[31] and, assuming that the allegations are verified, identifying measures to address reprisals and a devising timeframe for pursuing them. Measures should be discussed with the persons directly concerned or, when direct contact is not possible, with third parties that have the authority to represent the victims.

Examples

In line with its retaliation guidelines, the Inspection Panel informally develops a protection timeline on a case-by-case basis. This consists of internal discussions to identify protective measures in coordination with management and the requesters in response to retaliation. The Panel anticipates potential future scenarios and discusses appropriate responses and escalatory steps. Depending on the severity of the threats and with the agreement of the requesters, the Panel escalates it to different levels within management and in more serious cases also informs the World Bank Group President and the Board of Executive Directors. The Panel does that while ensuring the confidentiality of the requesters. Management usually takes the lead in the protective efforts and in raising the World Bank Group's zero tolerance approach to retaliation with its borrowers. Management also monitors threats and the borrower's actions in response to retaliation and keeps the Panel informed. The Panel communicates frequently with the requesters throughout the process to monitor developments on the ground.

Additional information about developing a protection timeline

While it is important for IAMs to gather and verify information and identify measures that should be taken, IAMs may need to respond to the allegations with immediate action, before verifying claims of threats or reprisals.[33] For example, if the person is in immediate danger, focus should be on reducing

31 - When requesters or their associates have experienced previous trauma or exposure to pressure, their perceptions of threats in the context of a given project could relate to the earlier incident or be exaggerated. In these situations, it is important for the IAM to gather and verify information about the allegations. Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons. pg. 29.

32- Ibid.

33 -Ibid.

the source of the threat, whether through direct engagement with the source, or by asking others to intervene.

As noted, the initial risk assessment should have considered the responses IAMs could take, alone or in cooperation with others, if reprisals occur. However, this initial assessment might not have accurately foreseen all instances of reprisals. Therefore, depending on the reported reprisal or imminent threat – including its nature, gravity, and impact on the persons concerned – IAMs might need to consider developing additional or new responses, and engage with new actors best placed to implement such responses.

SUGGESTED TOOLS

TOOL 1: Suggested template for a protection timeline template and guiding questions

According to the guidance provided by the UN Office of the High Commissioner for Human Rights[34] and other human rights mechanisms,[35] a protection timeline can be developed by taking the following actions:

1. Verify the facts surrounding the allegation of the reprisal.

2. Based on the nature and gravity of the reprisal and the capacities of the victim(s) to respond to the reprisal, assess if immediate action is required.

3. In consultation with the persons concerned, identify the best courses of action given the circumstances of the case, including a review of whether the previously-agreed responses to reprisals (done as part of the earlier risk assessment) are still relevant, and whether additional measures are needed.

4. Determine with the persons concerned how the measures will be put into practice, and by whom and when.

5. Monitor implementation, review and follow-up of the agreed measures.

6. Consider responses to the reprisal 'active' until it has been verified that the threat no longer exists, or that the risks have been reduced to an acceptable level.

These steps are elaborated next.

1. Verify the facts surrounding the allegation of a reprisal, including its objectives and severity

The following questions can help IAMs to verify allegations of reprisals, and assess their objectives and severity:[36]

- When and how was the threat received or communicated? What happened exactly?
- How did the person receive the threat? For example, does the person believe he or she is in danger because another person was threatened (perceived threat)?
- Was the threat direct (clearly and directly formulated), or was it implied by its source?
- If the threat is carried out, what are the possible consequences?

34 - UN Office of the High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and other cooperating persons. pgs. 29-51. See also Office of the UN High Commissioner for Human Rights: Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law (2015), pgs. 81–82.

35 - See, for example, UN Committee against Torture: Guidelines on the Receipt and Handling of reprisals against individuals and organizations cooperating with the Committee against Torture under articles 13, 19, 20 and 22 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. UN Doc. CAT/C/55/22 (September 2015); United Nations Human Rights Treaty Bodies: Guidelines against Intimidation and Reprisals (the San Jose Guidelines), UN Doc. HRI/MC/2016/6 (July 2015).

36 - See generally, Office of the High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, in particular pgs. 30–31. See also Eguren and Caraj, 2009. New Protection Manual for Human Rights Defenders (Protection International), pgs. 45–53.

- Is the source known? How much detail can be provided?
- Does the source of the threat have the capacity to act upon it? What are the possible political repercussions if the threat is carried out?
- What changed circumstances might trigger the source of the threat to retaliate?
- Can information about the reprisal/threat be verified by other independent sources?
- Have other persons also been retaliated against/threatened?
- What does the threat/reprisal intend to achieve (for example, for the person at risk to stop all communication with the IAM)? Is the threat/reprisal meant to hinder the IAM process?
- Are there any direct or indirect links between the source of the reprisal/threat and the national authorities or armed groups? If the source is a national authority, what is its position within the State apparatus?
- What is the past behavior of the source of the threat/other reprisal? What are its motives behind the act?
- Who may have influence or authority over the source of the threat/other reprisal for corrective action?

Understanding the source is key for designing appropriate measures to address the reprisal and reduce the level of threat. For example, if the source of the reprisal is a Government agency, IAMs can consider requesting intervention from senior leadership of the parent institution. If the source of the threat is a borrower/grantee taking part in an IAM-facilitated process, an intervention by the IAM itself may have a positive impact. If the source of the threat is an armed group over which neither the IAM, its parent institution, nor the Government has control, other actors, such as the UN Office of the High Commissioner for Human Rights or organizations providing protective accompaniment, may be better placed to address the situation.

2. Assess whether immediate action is required

IAMs have at least three possibilities to react to a reprisal:[37]

- An immediate reaction to stop/prevent a reprisal.
- If the incident is over, a rapid reaction, in the subsequent hours or days, to prevent possible new reprisals from arising.
- A follow-up action, in the subsequent days, weeks, or months, depending on the circumstances, if the situation has stabilized.

For each case, IAMs will need to decide whether immediate action is required to address the situation. This decision should be based on the nature and gravity of the threat/reprisal, and the capacities of the person(s) concerned to reduce the level of threat and respond to the reprisal. If in doubt, the IAMs should make their decisions based on the worst-case scenario.

When the pattern of threats increases in severity, it is an indication that the situation is increasingly dangerous.[38] As a rule, if the person is in imminent danger, IAMs should take immediate action, and focus on influencing the source of the threat.

When a serious reprisal has occurred – such as arbitrary detention, or physical violence – IAMs should also react as a matter of priority. The mapping of key actors that can provide protection (covered in the reprisals risk assessment) should be consulted, and updated as needed, in planning

37 - Eguren and Caraj, 2009. New Protection Manual for Human Rights Defenders (Protection International), pg. 49.

38 - Front Line Defenders, 2016. Workbook on Security: Practical Steps for Human Rights Defenders at Risk, pg. 28.

responses to immediate actions. An immediate reaction could, for example, entail requesting an intervention by the President of the parent institution or by international human rights mechanisms, as appropriate, for private or public diplomacy.

IAMs should always discuss with the persons concerned the immediate measures that could best respond to the situation and assess – to the extent possible – the potential consequences of these measures on the security of the persons at risk. [39]

3. Identify the best courses of action, how they will be put into practice and by whom

As noted, the initial risk assessment exercise should have resulted in an understanding with the person(s) at risk about the responses the IAMs could take, alone or in cooperation with others, if reprisals occur. However, the assessment may not be able to accurately foresee all instances of reprisals that may occur. Therefore, depending on the situation, IAMs may need to develop additional or new responses, and decide what actors would be the best placed to implement such responses.

Some measures IAMs can take include:[40]

- Intervening directly to influence or affect the behavior/attitude of the source of the threat.

- Engaging with an influential person, such as a religious, community, political, or civil society leader, who might be able to intervene with the source of the threat.

- Using visibility strategies as a deterrent effect: for example, IAMs and/or their parent institutions can issue public statements.

- Requesting the parent institution and/or President to engage with national authorities, stressing possible impacts of the reprisal.

- Seeking the support of relevant partners and international mechanisms, such as international or national CSOs, diplomatic missions, international or regional human rights mechanisms to build the capacity of the persons concerned for increased visibility to the case.

- Increasing political cost of retaliating by, for instance, requesting public statements from international or regional human rights mechanisms.

- Supporting self-protection strategies of the person(s) at risk, for example by facilitating temporary relocation initiatives through contact with appropriate CSOs or diplomatic missions.

In addition, IAMs should discuss with the persons at risk how the agreed measures will be put into practice, when, and by whom. In devising the most appropriate response and in consultation with the person(s) at risk, IAM should also consider measures that should follow a sequence, and those that should be taken in parallel.[41] For example, the person that has received a threat or been the victim of a reprisal may prefer to address the situation first, before wanting the IAM and/or its parent institution to raise the case with national authorities.[42] Alternatively, the response can be carried out at different levels at the same time, for example, by supporting the person to connect with protection networks that can offer

39 - See Guidelines against intimidation or reprisals adopted at the twenty-seventh meeting of chairpersons of the human rights treaty bodies (San Jose Guidelines). UNs Doc. HRI/MC/2015/6 and the Special Procedures of the UN Human Rights Council: Enhanced Response to Acts of Intimidation and Reprisal for Cooperation with the Special Procedures (http://www.ohchr.org/EN/HRBodies/SP/Pages/Actsofintimidationandreprisal.aspx)

40 - Adapted from Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, pg. 32.

41 - Ibid.

42 - Ibid.

temporary relocation solutions, while intervening with national authorities or others than can have positive influence over the situation.[43] It is of paramount importance that both the IAM and the person at risk acts in accordance with earlier understandings.[44]

4. Work closely with the person(s) at risk and relevant partners to implement the measures, and ensure regular communication, review, and follow-up

It is important to establish check-in routines for staying in regular contact with the person(s) concerned, or, where direct communication is not possible, with the organization or individuals that have the authority to represent them. Regular communication becomes essential as levels of risk rise.[46] For that purpose, IAMs need to establish, as part of their protection timeline, how to communicate with the person concerned (for example, directly or through third parties) and agree on the timing for doing so. Provisions should also be made for unexpected breaks in communication when the IAM is no longer able to contact the persons concerned. This will enable the IAMs to find out the reason for this lack of contact to decide on further action.

Implementing agreed measures also requires continuous communication between all parties involved. For example, if the best course of action requires the IAM to temporarily halt the investigative process and engage with its parent institution to raise the case with national authorities, while the affected person goes into hiding, it is imperative that all three parties keep the lines of communication open and provide regular updates on actions taken and responses received. Where one or more parties fall short of communicating, the person at risk may make bad judgment calls and take new risks to address concerns.

5. Determine that the threat no longer exists, or the risk has been minimized to an acceptable level

IAMs should maintain their protection timeline active until the persons at risk, or others with the authority to represent them, clearly communicate that there is no longer an immediate threat.[46] IAMs should always be able to justify why the timeline is no longer considered to be active.

TOOL 3: Actors that can be approached for support in implementing the protection timeline

IAMs have a limited mandate and scope of action once reprisals have occurred, and they are largely dependent on approaching other actors who may be able to act to provide protection or other measures to reduce the level of threat and impact. These include:

- Management of the IAMs' parent institutions
- Decision-makers of the IAMs' parent institutions (President and Board)
- International and regional human rights mechanisms
- Diplomatic missions
- National protection mechanisms
- Nongovernmental organizations and networks specialized in the protection of individuals and groups at risk.

The appendixes include examples on the kind of support IAMs could seek from these actors and how they could be approached. They also include information on suggested resource organizations that can support the implementation of strategies to reduce risk.

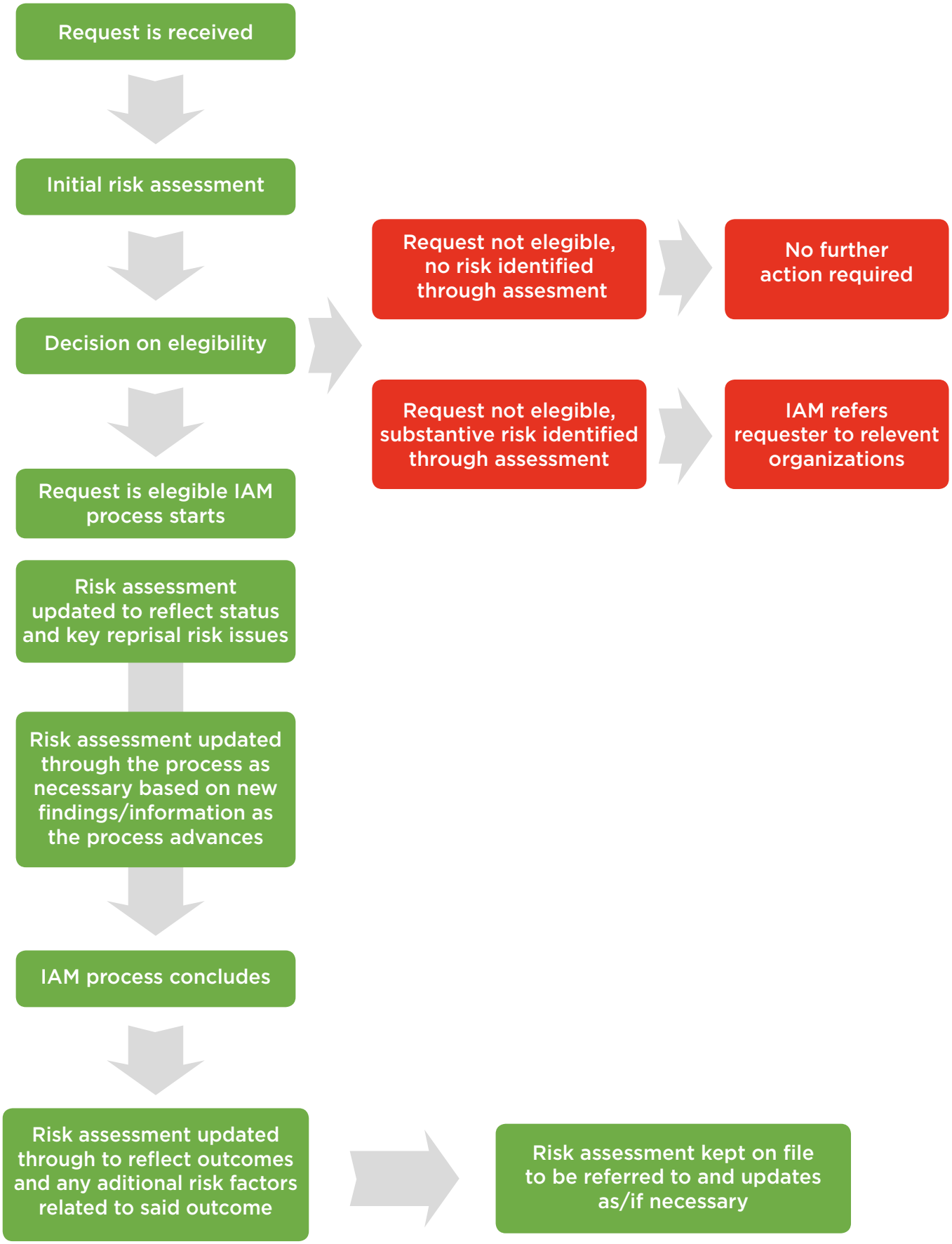
43 - Ibid.

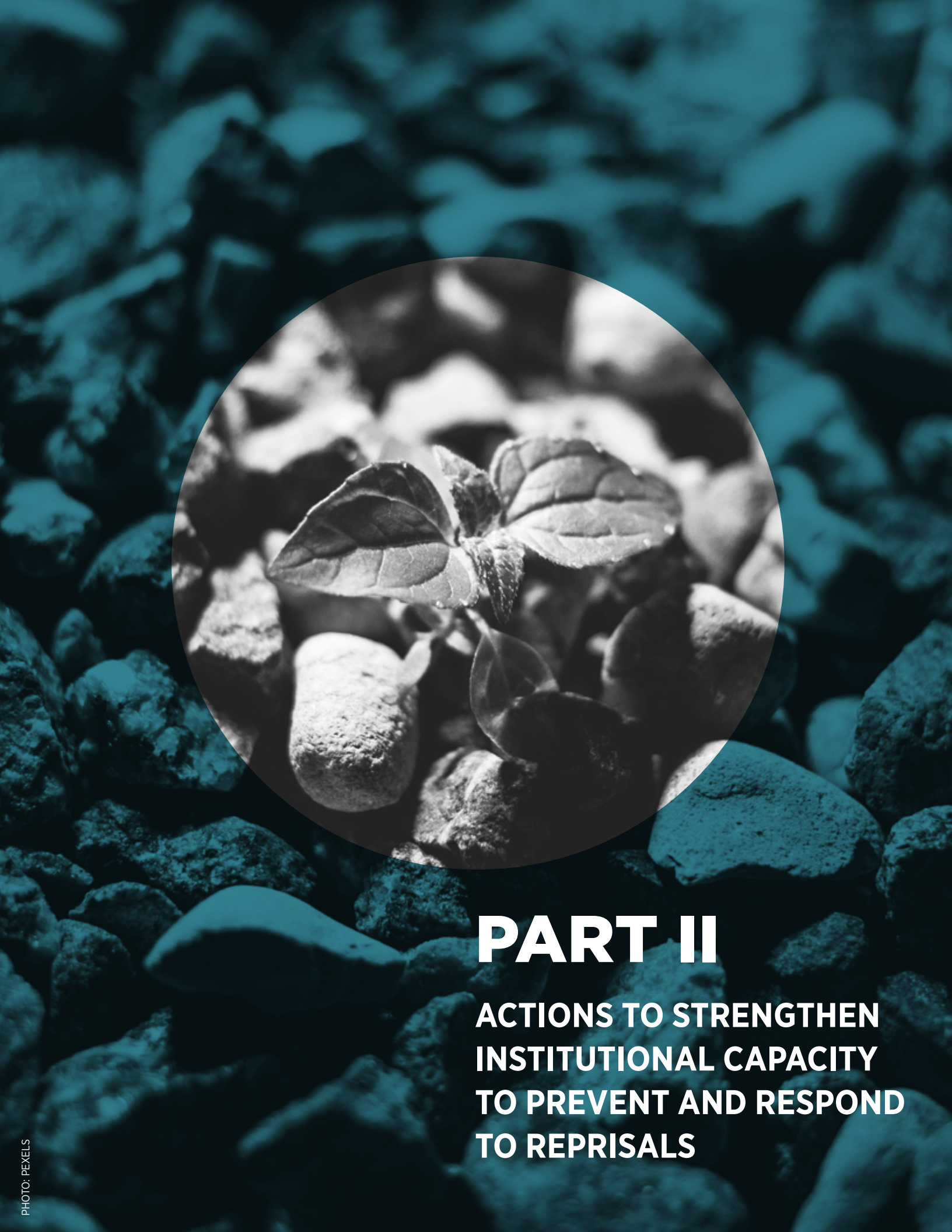
44 - Adapted from Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, pg. 32.

45 - International Service for Human Rights: Reprisals Handbook, 2018.

46 - Ibid.

Timeline and Action for Risk Assessment Flowchart





PART II

ACTIONS TO STRENGTHEN INSTITUTIONAL CAPACITY TO PREVENT AND RESPOND TO REPRISALS

PHOTO: PEXELS

ESTABLISHING SAFER LINES OF COMMUNICATION

When establishing safer lines of communication with requesters and other related stakeholders, as well as additional measures that could better ensure privacy of communications and identity protective measures that could be taken throughout the IAM process, IAMs should consider the following two Actions:

- Address risks related to first contact with IAMs through the mechanisms' parent institutions
- Assess and address risks inherent to IAMs' standard digital communication systems

ACTION 12: ADDRESS RISKS RELATED TO FIRST CONTACT WITH IAMS

What it is

IAMs are advised to assess and address risks of reprisals that relate to first contact from requesters. Risks have been identified both for traditional and digital means of communication.

Why it is important

Interviews with IAMs and civil society organizations have identified several challenges for IAMs to ensure the privacy of first contact from potential requesters. If first contact from requesters – whether traditional or digital communication – is intercepted, it can significantly jeopardize their security and impose later challenges in keeping their confidentiality.

SUGGESTED TOOLS

TOOL 1: Allowing first contact directly with IAMs; seeking modification to the possibility for first contact through IAMs' parent institutions.

Many IAMs and CSOs have expressed concern about early contact through the country office of the IAMs' parent institutions, particularly in the case of those IAMs that require requesters to contact management before going to the mechanisms. Engagement by Management with the requesters, or redirecting them to the executing agency, requires the exposure of the identity of the complainants, and can pose unnecessary risks of reprisal even before the IAM has been made aware of the request.

To provide greater safeguards to requesters, IAMs could seek to raise awareness of this risk to the President or the Board of the parent institution and seek a waiver from this requirement.

TOOL 2: Encrypt online complaints/contact forms

Several of the IAMs have online contact and complaints forms that can easily be filled out and submitted by requesters or supporting organizations with access to internet. IAMs that currently offer online complaints forms, or are in the process of developing such forms, are encouraged to consider how to protect the system from external interference.

The Internet is an open network through which information generally travels in a readable format.[47] If the submission of a request through an online complaints form is intercepted on its way to the IAM, its contents can be easily read by others.[48] Thus,

47 - Bogusz, Vitaliev, and Walker, 2009–present, Security-in-a-box (for Tactical Technology Collective and Front Line Defenders). https://securityinabox.org/en/guide/secure-communication

48 - Ibid.

external actors may have access to information that can motivate reprisals and can easily locate the requesters through the contact information that has been provided by the requesters in the contact or initial request forms.

An important way to ensure that the contents of an online complaint form cannot be intercepted is to encrypt the forms. In simple terms, encryption is a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient,"[49] and it protects the confidentiality and integrity of the content against third-party access or manipulation. In the IAM context, encryption would mean that the requesters' responses are encrypted in the browser of the person filling out the form and cannot be seen by any entity other than the IAM.[50]

IAMs may wish to work with the IT teams of their parent institutions or work with external organizations with expertise in the field of digital security.[51]

However, in some countries, using encrypted communications is illegal and/or a punishable crime. In these situations, IAMs should also consider maintaining a non-encrypted form as an alternative.

Examples

The Project Complaints Mechanism of the European Bank for Reconstruction and Development has taken the lead in addressing (digital) risks related to first contact from requesters.

The Compliance Advisor Ombudsman has also noted that the option of a secure online platform will be considered in its upcoming update of its website and has stated a commitment to using encrypted mediums for communication and other technological best practices to help safeguard confidentiality online and in relation to other types of communication systems.

TOOL 3: Encourage potential requesters to think about their digital security

Requesters and other related stakeholders often disregard digital safety. Therefore, IAMs may wish to include in their online contact and complaints forms an alert that can help requesters assess whether communication with the IAM can put them at risk – and prompt them to, at a minimum, use a secure computer and a safe internet connection, and open, and provide an address for, a separate, new email account.

The secure grant form (https://frontlinedefenders.org/secure/grant.php) of the CSO Front Line Defenders is a model to consider as it underscores the importance of thinking about digital security when filling in and sending the form. It also emphasizes the user's responsibility to take additional measures to ensure his or her own safety by noting that:

"If you feel that contact with Front Line Defenders may put you at risk we suggest that at minimum you use a secure computer, safe Internet connection and open a separate, new email account and provide this address in the application instead. For further information, see Keep your online communication private" (https://securityinabox.org/en/guide/secure-communication/) and "Communicating with Others" (https://ssd.eff.org/en/module/communicating-others)"

49 - See SANS Institute: "History of Eencryption," 2001, as referenced in the report of the UN Special Rapporteur on the promotion and protection of the right of the right to freedom of opinion and expression, by David Kaye (May 2015). UN Doc. A/HRC/29/32, paragraph 7.

50 - By way of simplification, a secure (encrypted) online complaint form is a simple PHP script (program). When a requester opens the online complaints form in her/his browser, s/he does so over an encrypted (SSL) connection between the IAM's server and her/his internet browser. The responses are written by the requester and are sent over the same encrypted connection to the IAM's website where another PHP script receives the text, encrypts it, and passes it on to a predefined email address.

51 - See, for example, Front Line Defenders secure contact forms and the forms provided by protectdefenders.eu.

ACTION 13: ASSESS AND ADDRESS RISKS RELATED TO STANDARD DIGITAL COMMUNICATION SYSTEMS

What it is

IAMs may wish to consider systematically assessing and addressing risks related to their standard digital communication systems.

Why it is important

Digital alternatives to traditional means of communication cannot always be relied upon to keep sensitive information private. Most of the commonly used webmail and instant messaging services, for example, do not ensure privacy of communication.[52] In part, this is because a few powerful computers can automatically search through a large amount of digital information and identify senders, recipients, and specific key words, while much greater resources are needed to carry out the same level of surveillance of traditional communication channels.[53] If the IAMs or other stakeholders rely on emails, instant messaging, or voice over internet protocol conversations (such as Skype) and do so using insecure methods, the communication is almost certainly less private than letters or telephone calls.[54]

Contemporary digital technologies allow an unprecedented capacity to intercept communication, and individual persons and human rights organizations are increasingly subject to digital surveillance.[55] This trend will pose growing risks to ensure safe online communication with requesters, complainants, and other cooperating persons.

Example

The Project Complaint Mechanism (PCM) of the European Bank for Reconstruction and Development (EBRD) has taken the lead in working to address systematic challenges to ensure privacy of communication to and from requesters and others. Working with the IT department of its parent institution, the PCM is in the process of developing an encrypted online complaint form and a secure cloud to share documents with its external consultants. A secure chat function is also in the pipeline.

To assess the level of security of the EBRD's communication systems, it has worked with ethical hackers - computer and networking experts who systematically attempt to penetrate a computer system or network for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit.

Additional information about the risks inherent in the digital communication procedures of IAMs

Among the challenges observed to ensuring privacy of communication in the IAM context:

- IAMs and their parent institutions do not rely on secure socket layers and can therefore not ensure a secure internet connection and the privacy of those that visit the sites (and potentially submit online complaints).
- IAMs do not provide a secure file share system and regularly communicate highly sensitive information to other staff and external consultants through emails or USB keys, or use the same file share systems for all information (including information that should be highly restricted in terms of access).

52 - Bogusz, Vitaliev, and Walker, 2009–present, Security-in-a-box (for Tactical Technology Collective and Front Line Defenders), https://securityinabox.org/en/guide/secure-communication.

53 - Ibid.

54 - Ibid.

55 - There is a growing trend in targeted digital attacks against civil society and human rights defenders. According to information provided by the CSO Front Line Defenders, intrusive spyware has been in use by Governments in at least 42 countries. See https://www.frontlinedefenders.org/en/resource-publication/living-under-digital-surveillance for additional information.

- IAMs communicate with requesters and other stakeholders associated with the IAM process (such as national facilitators and experts) through WhatsApp or other chat functions whose security is entirely dependent on the user.

- IAMs and their parent institutions have not established or made mandatory training programs on how to safely work with digital communication tools. Thus, staff and others associated with the IAM process have limited, or partial, awareness about how to ensure privacy of communication when working with digital communication tools (including smartphones and commonly used applications).

SUGGESTED TOOLS

TOOL 1: Conduct a digital security audit

This toolkit is not intended to be a technical guide to digital security. Digital security is a highly complex topic, and as tools for communication are constantly evolving, as are the different ways to intercept them.[56] Each IAM will also face unique challenges in ensuring the privacy of its online communication with requesters. Therefore, IAMs are encouraged to work with the IT department of their parent institutions or (if feasible) with external expert organizations, to conduct a digital security audit to better understand and address inherent risks in their current standard operating programs and procedures used for communication. Such an audit can identify specific challenges each IAM faces to ensure secure communication channels, and the measures needed to reduce risks.

Should there be concerns about consulting within the institutions, IAMs could also liaise with CSOs that have specific expertise in digital security for human rights defenders such as Tactical Technology Collective, Front Line Defenders,[57] and Surveillance Self-Defense.[58] These organizations have produced quality and accessible resource materials on digital security.

TOOL 2: Further reading

IAMs may find it useful to suggest that requesters research the following sources:

- **Surveillance Self-Defense (SSD)** is a guide to protecting users from electronic surveillance. Some aspects of this guide will be useful to people with limited technical knowledge, while others are aimed at an audience with considerable technical expertise and privacy/security trainers. SSD includes step-by-step tutorials for installing and using a variety of privacy and security tools, but also aims to teach people how to think about online privacy and security in a sophisticated way that empowers them to choose appropriate tools and practices, even as tools and threats change around them.

- **Security in a Box** was created by Front Line Defenders and Tactical Tech in 2009 to meet digital security and privacy needs of human rights defenders. Since then, the website has been updated and expanded to keep up to date with a rapidly changing digital environment. It is available in 17 languages: Amharic, Arabic, Bahasa, Burmese, Chinese, English, Farsi, French, Khmer, Macedonian, Portuguese, Russian, Spanish, Thai, Tibetan, Turkish, and Vietnamese.

Security in a Box includes:

A How-to Booklet covering 11 areas, including "how to protect your computer from malware and hackers" and "how to protect the sensitive files on your computer."

Hands-on Guides, each focusing on a specific

56 - Bogusz, Vitaliev, and Walker, 2009–present, Security-in-a-box (for Tactical Technology Collective and Front Line Defenders) https://securityinabox.org/en/guide/secure-communication.

57 - Ibid.

58 - Surveillance Self Defense – a project of the Electronic Frontier Foundation: Tips, Tools and How-to's for Safer Online Communication. https://ssd.eff.org/en/

freeware or open source software tool. Each Guide shows users how they can use that tool to secure their computer, protect their information, or maintain the privacy of their communication.

A Mobile Security section, showing users how to install and use specific freeware or open source smartphone applications, helping to make their smartphone use more secure.

- **Digital Security First-Aid Kit for Human Rights Defenders** (second edition), produced by the Association for Progressive Communication, contains short guides for human rights defenders who find themselves in emergencies related to communication and digital security. The kit suggests concrete steps, as well as providing further resources and references to support groups to whom activists can turn for further assistance.

- **Rise Up** provides online communication tools for people and groups working toward social change, with a focus on providing resources and tools for safer communication.

- **¡Pongámonos las Pilas!** (available only in Spanish) seeks to provide the basis for an information security policy for organizations, particularly in relation to digital security.

- **Me and my shadow**, by Tactical Technology Collective, outlines many of the ways in which users leave traces of their personal information online. It includes advice and information about staying safe in the digital world, as well as links to useful online resources.

- **Electronic Frontier Foundation** provides detailed info on dealing with Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which aim at preventing a website from functioning properly.

PHOTO: TWITTER GREENPEACE

Gloria Capitan,
Philippines.

ENSURING CONFIDENTIALITY THROUGHOUT THE IAM PROCESS

Maintaining confidentiality when handling cases can be one of the most effective ways to prevent reprisals.

All members of the IAM Network currently provide for the right of requesters and associated persons to have their names and personal information kept confidential and strictly within the IAMs.

The research for this toolkit has identified several challenges to ensure that confidentiality is maintained throughout the process. Therefore, the toolkit suggests additional actions to consider to better ensure that identity of individuals and groups at risk of reprisal, and sensitive information they provide, are protected throughout the IAM process.

The suggested actions include:

- Informing requesters and other related stakeholders about the possibilities of and challenges to IAM's ensuring their confidentiality
- Seeking modification to requirement for prior engagement with parent institution management/fund recipients/clients/subclients
- Ensuring that confidentiality is maintained throughout the problem-solving process.
- Reducing exposure to risk in the context of IAM field visits.
- Ensuring the safe handling of sensitive information.

ACTION 14: INFORM REQUESTERS AND OTHER RELATED STAKEHOLDERS ABOUT THE POSSIBILITIES OF AND CHALLENGES TO IAMS ON ENSURING THEIR CONFIDENTIALITY

What it is

IAMs are encouraged to seek to understand whether the requesters and other related stakeholders are putting themselves at unreasonable risk of reprisals if confidentiality is not maintained.

Where requesters have not asked for confidentiality, IAMs may wish to consider proactively informing them about risks of reprisal and their right to have their identities and the sensitive information they provide kept confidential and ask them to reconsider their decision. Ultimately, requesters' choice should be respected, as visibility might be part of their overall security strategy.

To ensure that all parties reduce risks of having identities of individuals at risk exposed, the mechanisms may also wish to clearly inform them, at the earliest stage of the process, about the mechanism's possibilities of, and challenges to, ensuring confidentiality throughout the process.

Why it is important

When individuals request confidentiality, it is usually a sign that there have been, or may be, reprisals, and that precautionary measures, including respect for confidentiality, need to be taken to reduce those risks. Nevertheless, the fact that some requesters do not ask for confidentiality cannot be taken to mean there are no risks. Requesters may not be able to make a judgment about the need for

confidentiality because they are overconfident, in denial, or underestimate the risks of the situation, or simply because they lack information[59] about the possibility that they can request confidentiality.

SUGGESTED TOOLS

TOOL 1: Adopt a public policy and associated internal guidelines on how the IAM ensures confidentiality, and their limitations to protect the identity of requesters, complainants, and other associated persons

IAMs could adopt a policy on confidentiality that they can disseminate to their members and support staff and share with requesters, complainants, and others with whom the IAMs interact.[60] Alternatively, confidentiality could be part of the guidelines IAMs are encouraged to develop for addressing reprisals.[61]

Whatever format IAMs choose to communicate how they safeguard the right to confidentiality, it is important to address how they will ensure confidentiality of both the identity of those with whom they interact and of the information provided.[62] They should also specify possible limitations to ensuring respect for confidentiality (for example, with regard to disclosure of information to parent institution management and other IAM staff).

TOOL 2: Suggested template for a policy on confidentiality

The guidance by the UN Office of the High Commissioner for Human Rights for developing policies on confidentiality is a useful model to consider. According to this guidance:

- All victims, witnesses, and other persons cooperating must be informed of the policy on confidentiality[63] before being requested to provide information on incidents or cases of individuals facing threats or harm because of their interaction [with the UN field presence].

- Confidentiality covers the identity of the cooperating person and the information they provide (including audio and video recordings, photographs, and other types of documentation), unless specific consent has been given for their use.

- Confidentiality regarding protection cases also covers information on the protective measures taken, including any support given by external parties. This is essential to guarantee the safety not only of the person benefited from the measures, but also of others who may benefit from them in the future.

- Victims, witnesses, and other cooperating persons need to give their informed consent for the use of information provided. The consent should be specific: for example, consent to report information only internally or to report information publicly with or without revealing the identity of the source.

- Additional efforts should be made for children, persons with disabilities, or persons who may not be sufficiently familiar with concepts such as confidentiality and consent, to ensure that the person(s) concerned understands these concepts and provide(s) informed consent.

59 - Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, pg. 7.

60 - Ibid., and Office of the UN High Commissioner for Human Rights: Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law (2015), pg. 75

61 - The guidelines on preventing and addressing reprisals that have been adopted by the Inspection Panel and the Compliance Advisor Ombudsman cover, in part, the right to confidentiality.

62 - Office of the UN High Commissioner for Human Rights: Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law (2015), pg. 75

63 - Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, pgs. 7–8.

- Confidentiality will be respected regardless of the conditions in which the information was obtained – whether confidentiality was explicitly requested by the cooperating person, was implied, or was guaranteed, explicitly or otherwise. If the conditions under which the information was provided are unclear, the identity of the person and the information provided should be considered confidential until specific consent is given for the use of the information.

- Even if consent is granted to disclose information publicly or to a third party, potential implications of doing so should always be assessed. If there is a risk of harm, information should not be disclosed, or should be disclosed in a manner that reduces the risk (such as providing information on a general pattern without revealing specific details).

In line with practice of international human rights mechanisms, IAMs are also advised to develop additional internal staff guidelines on how to preserve confidentiality of sources of information and the measures in place to do so.[64]

The Human Rights, Methodology, Education and Training Section of the UN Office of the High Commissioner has worked extensively on the question of confidentiality in the context of sensitive missions, including commissions of inquiry and fact-finding missions.

ACTION 15: ADDRESS RISKS RELATED TO CURRENT REQUIREMENTS FOR PRIOR ENGAGEMENT WITH PARENT INSTITUTION MANAGEMENT/FUND RECIPIENTS/CLIENT

What it is

For a request to be considered eligible, policies of some IAMs require that requesters have first approached management of the IAMs' parent institutions with their concerns and have not been satisfied with the outcome.[65] This requirement has been set in the belief that most of the issues may be best resolved at the project level. However, in some cases where risk of reprisals exists, the IAMs may want to seek modification to the requirements that requesters need to approach management/the fund recipient/client with their concerns before submitting a claim to the IAMs. The policy/procedure review process of IAMs presents an important opportunity to discuss this issue through the lenses of reprisals.

Why it is important

When requesters satisfy this requirement, management of the IAMs' parent institutions are aware of requesters' identities by the time the case is received by the IAMs and may also have informed the project implementing agency in (well-intended) efforts to resolve the problem early on. As such, it is easy to trace back a complaint to an individual or group once it becomes known that a case has been received by the IAM, which undermines the possibility of ensuring confidentiality later down the line.

SUGGESTED TOOLS

TOOL 1: Consider waiving the requirement for prior engagement in situations in which there is a risk of reprisal

IAMs may wish to consider lobbying for policy modifications to ensure that the eligibility of a request does not hinge on requesters having communicated their concerns to Management (or fund recipient) first, when they perceive that doing so could put them at risk of reprisal.

64 - Office of the UN High Commissioner for Human Rights: Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law (2015), pg. 73. Such measures may include exclusive use of a dedicated IAM database to collect, document and store information while on field missions and password protection, as discussed in this toolkit.

65 - This is the case with, for example, the World Bank's Inspection Panel, the Independent Consultation and Investigation Mechanism (MICI) of the Inter-American Development Bank and the Complaints Mechanism of the Asian Development Bank, which all require that the concerns of the requesters have been brought to the attention of Management of the IAMs' parent institutions.

Some of the IAMs do not require that requesters communicate their concerns to parent institution management and/or the fund recipient (borrower/client). For example, the Project Complaints Mechanism (PCM) of the European Bank for Reconstruction and Development (EBRD) specifies in its online complaint form that requesters can explain why they have not contacted the parent institution and/or fund recipient/client to try to resolve instances of harm or expected harm.[66] This provision is also considered in the policy of the Independent Consultation and Investigation Mechanism (MICI) of the Inter-American Development Bank (IDB).[67]

ACTION 16: ENSURE CONFIDENTIALITY DURING THE PROBLEM-SOLVING PROCESS

What it is

IAMs have observed that ensuring confidentiality is particularly challenging during the problem-solving phase. This is because mediation is a voluntary endeavor in which the consent of all parties is critical for a viable process and a durable outcome.[68] When one of the parties is asking for confidentiality, the consent of the other party or parties will be hard to obtain.

Why it is important

If the confidentiality of the persons at risk of reprisal is not guaranteed during the problem-solving phase, it may not only generate more risk to the requesters, but also invalidate the possibility of ensuring confidentiality during later stages of the IAM process (such as compliance review and monitoring) should the mediation fail.

SUGGESTED TOOLS

TOOL 1: Shuttle diplomacy

Shuttle diplomacy, also known as mediated communication, can be useful in these types of situations, at least in the early stages when direct communication may provide fertile ground for reprisals.

The essence of shuttle diplomacy is the use of the IAM, as a third party, to convey information back and forth between the parties, serving as a reliable means of communication.[69]

When requesters ask for confidentiality, or when an early assessment of the request suggests that reprisals are likely, and risks cannot immediately be reduced, IAMs may wish to consider shuttle diplomacy as a viable action for part or all the dispute resolution phase.

ACTION 17: REDUCE EXPOSURE IN THE CONTEXT OF IAM FIELD VISITS

What it is

Ensuring confidentiality requires the exercise of good judgment and caution by IAM staff and facilitators in all their interactions with requesters and others associated with them. Therefore, an important consideration for IAMs is how to reduce the likelihood that interactions with requesters and other related stakeholders are made known before, during, and after field visits.

Why it is important

Lack of care to conceal contact can significantly increase the risk of reprisals for requesters and other local stakeholders.

Additional information about risks relating to field visits

In the context of field missions, both IAM staff and external resource organizations have noted that, in some cases, sharing information with parent institution management and decision-makers about mission dates may increase the risk of reprisals to those with whom the mechanisms interact.

66 - http://www.ebrd.com/eform/pcm/complaint_form?language=en.

67 - See Policy of the Independent Consultation and Investigation Mechanism of the IDB, paragraph 22 (d).

68 - United Nations, 2012 Guidance for Effective Mediation – issues an Annex to the report of the Secretary General on Strengthening the role of mediation in the peaceful settlement of disputes, conflict prevention and resolution (A/66/811, 25 June 2012), pg. 4.

69 - Burgess and Burgess, 2003. Shuttle Diplomacy/Mediated Communication, University of Colorado.

The current policy at most parent institutions is to inform parent institution management and the Board about planned missions. Dates may be discussed and agreed with the country office of the IAMs' parent institutions and IAMs might also need to contact their parent institution security team in order to make a security assessment and arrangements for the mission.

Providing information can increase risks of surveillance of IAM staff (and related experts and facilitators) during the country visit. When IAM staff are under surveillance, their meetings with requesters and others may put at risk their requests for confidentiality. Notwithstanding these limitations, there are measures IAMs could consider to mitigate risks.

SUGGESTED TOOLS

TOOL 1: Conduct separate field visits where risks of reprisals have been identified

IAMs could consider conducting two separate missions: first, to engage only with parent institution management and other relevant actors (such as the project implementing agency and other associated Government authorities). Detailed agenda and dates for this mission would be shared with the Board, parent institution management, and/or fund recipients/client in the country concerned. A second mission for which specific dates and agendas are confidential could be used to meet solely with requesters and others associated with them.

TOOL 2: Codify current good practice relating to staff conduct in the field

Several IAMs have established good practice for ensuring confidentiality in the context of field missions. To organize and preserve this institutional memory, IAMs could codify current good practice into internal guidelines for staff and others that facilitate IAM processes.

Current best practice of specialized mechanisms and organizations working with individuals and groups at risk suggests that a code of conduct would benefit from reflecting the following key issues:[70]

- **Choosing the most appropriate meeting venue**

Finding the best venue to meet with requesters, complainants, or others associated with them is one of the most important aspects of minimizing exposure to risks of reprisal. An ideal meeting venue should be able to protect the identity of the interviewees and guarantee their safety and confidentiality of the information they provide.[71] When choosing the meeting place, IAMs will also need to consider whether the space will be used by several groups at the same time, and if so, have information about these groups and their relationship to the interviewees.[72]

The meeting venue should be decided in advance with requesters and other relevant stakeholders. While the final decision about meeting venues should be based on a discussion with the persons concerned, IAMs are encouraged to also consider the views of local civil society organizations and other country-based mechanisms with experience in protection measures, such as local UN Human Rights Offices.[73] If the location suggested by those at risk poses risks of harm that the persons concerned are not aware

70 - The following section draws heavily on the guidance by the Office of the UN High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, and the manual produced by the Tactical Technology Collective: Holistic Security – Trainer's Manual (2017).

71 - UN High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, pg. 16.

72 - Tactical Technology Collective, 2017. Holistic Security – Trainer's Manual, pg. 17.

73 - UN High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, pg. 16.

of, or are disregarding, IAMs should propose alternative, safer venues.[74]

By way of example, a hotel is generally not considered a safe meeting place as conversations can be easily overheard, and/or video cameras or other surveillance equipment may jeopardize confidentiality of discussions. A better action may be to meet in the house of a friend of the complainant(s) that is located outside the immediate conflict area (the project area). If only public spaces are readily available for the meeting, a busy fast food café where the tables are not preassigned is the safest action.[75] A public park might also be safe, but it is important to keep walking and be aware of others trying to listen in to the conversation.[76] When meetings are held in public spaces, requesters and other stakeholders will need to take additional measures to minimize risks of reprisals. For instance, if it is decided that a meeting will take place in a shopping mall and the complainants come from an indigenous community, it could be agreed in advance that they do not come to the meeting dressed in their traditional clothing, as this may bring unwanted attention to them and the meeting.

IAMs are encouraged to always discuss and agree with the persons concerned an alternative for meeting locations, in case something goes wrong, and the original location can no longer be used.[77]

At times, the situation may also warrant that the persons concerned are informed of the location of the meeting at the last moment, to minimize chances of surveillance.[78] Encouraging diversion techniques, such as randomly riding around town until it can be established with certainty that no one is following, may be a required complementary measure.[79]

• Agreeing on ground rules for meeting(s)

IAMs could discuss and agree with requesters who may be allowed to attend the meeting, and what measures should be taken if unwanted individuals interfere.[80] Agreeing in advance on who can and cannot attend meetings is particularly important when communities are divided over the project under review and the IAM intervention, and other community members may retaliate. Ensuring that unwanted persons are not around during the interviews also ensures better confidentiality, and reduces the chances that others report the interview, with possible consequences for the interviewed.[81] In addition, interviewees should not be forced to share their real names, or any other details if a threat of infiltration exists.[82]

IAMs are also encouraged to agree with the persons concerned on protocols for recording and sharing information before, during, and after the meeting. Agreeing on the use of electronic devices and connectivity is especially important: while access to electronic devices may be very important for participants who wish to follow

74 - ibid. Note that this is the approach also taken by the World Bank's Inspection Panel which, in its guidelines to address risks of reprisals, emphasizes that the Panel favors the choice of meeting locations suggested by requesters. However, if the Panel deems the location to be risky, it suggests alternative locations and/or proposes phone meetings or secure-correspondence exchanges.

75 - Front Line Defenders, 2016 Workbook on Security: Practical Steps for Human Rights Defenders at Risk, pg. 75.

76 - Ibid.

77 - Tactical Technology Collective, 2017. Holistic Security – Trainer's Manual, pg. 18.

78 - See examples provided by the UN High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, pg. 17.

79 - Ibid.

80 - Tactical Technology Collective, 2017. Holistic Security – Trainer's Manual, pg. 18.

81 - See examples provided by the UN High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, pg. 17.

82 - Tactical Technology Collective, 2017. Holistic Security – Trainer's Manual, pg. 18.

developments at home or keep in touch with friends and relatives, the potential for surveillance should be flagged and agreements should be established about when and where it is acceptable to store and use devices.[83] No participant should be forced to have anything they say or even their presence at the event shared by another participant without their permission. In this regard, the use of social media usage should also be discussed.[84]

IAMs may wish to regularly "check in" with requesters/complainants/other cooperating persons on anything that is happening outside of the meetings and give them space to share any security incidents they may have noticed in the immediate surroundings of the meeting venues.[85]

During the interview, IAMs and the interpreter, if present, should never refer explicitly to statements made by others.[86] Such an error may endanger previous contacts and make the interviewee concerned about confidentiality of information he or she provides.[87] The identity of others with whom the IAMs have interacted should never be revealed, even if the IAMs were referred to the interviewee by one of them.[88]

IAMs are encouraged to discuss with the interviewees appropriate methods to keep in touch and arrange for a follow-up call or face-to-face meetings where possible.[89]

- **Blending in: Travelling unnoticed**

It is often challenging for IAM staff to go unnoticed when travelling to a neighborhood, community, or region where foreigners rarely venture. Without undermining their own security, there are several ways for IAM staff to "blend in", such as:

- Planning an interview with a wider number of individuals in the same community (even if irrelevant to the IAM case), so as to not single out the person they want to contact.[90] There is some safety in numbers and it is easier to retaliate against one individual than against many. Nonetheless, it may be possible that all those who were contacted will suffer reprisals or that one person in the community is subjected to harm to discourage or scare off others from cooperating with IAMs.[91]

- Not being vocal about the purpose of the visit to a certain location or the person they are meeting/interviewing, and never discussing the mission in places where they can easily be overheard, such as in hotels, restaurants, taxis, or other public transport.[92]

- Parking vehicles at a distance from the agreed meeting location, or at a different location where it is less visible, and walking to the venue of the meeting/interview.[93]

83- Ibid.

84 - Ibid.

85 - Ibid.

86 - UN High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons, pg. 17.

87 - Ibid.

88 - Ibid. The only exception would be if those contacts had given specific consent for their identity to be disclosed.

89 - Ibid., pg.18. This is the approach also taken by the World Bank's Inspection Panel which, in its guidelines to address risks of reprisals, emphasizes that the Panel proposes follow-up meetings or conversations and suggests appropriate methods for doing so.

90 - Ibid., pg. 16.

91 - Ibid.

92 - Ibid.

93 - Ibid.

- Requesting trusted intermediaries, such as CSOs or other community-based leaders, to facilitate the meeting/interview by contacting the person(s) concerned and accompanying him/her/them to the agreed meeting venue.[94]

- Entering the meeting venue beforehand, and separately from those with whom they will meet.[95]

- Trying to blend in with the local environment as much as possible, for example by travelling as a team of one female and one male IAM staff/expert to give the impression that they are a couple on a tourist visit.

- Ensuring that IAM team members do not travel together and are never seen in public together. This can be done through taking different routes when travelling, staying in separate hotels, and clearly dividing tasks so that one of the team members meets only with parent institution management/project implementing agency/Government authority, while the other only meets with requesters and others associated with them.

- Note that the need for these measures will depend on the case; some cases will require only some of these measures, or none of them.

• Ensuring that national facilitators understand the need for confidentiality and act accordingly.

National facilitators need to be recruited with great care. IAMs should pay particular attention to the selection of interpreters, who interact directly with requesters, complainants, and other sources, and who have access to confidential and sensitive information in doing so.

The assessment of the suitability of suggested facilitators for the IAM field visits should include checks on any past political involvement, affiliation, or link with authorities, political parties, opposition groups, or other similar entities, or any other ties that can indicate political or ethnic bias.[96] For example, the general practice of the UN Human Rights Office in Nepal was to not recruit national staff from the area where they were expected to work. This practice was meant not only to protect national staff from being exposed to risks of reprisals, but also to better guarantee impartiality and independence in the context of their work.[97] Past employment with parent institutions of the IAMs should also factor into recruitment decisions. As a rule, IAMs are encouraged to not hire interpreters, drivers, or other support staff that have worked or currently work for the IAMs' parent institutions.

Because of the nature of their work, interpreters usually have access to confidential and sensitive information. Interpreters need to be briefed on the nature of the IAMs' work and their role in ensuring respect for confidentiality of requesters/complainants or other sources and of the information they provide,[98] and should be required to sign confidentiality clauses as part of the recruitment process.

ACTION 18: ENSURE THE SAFE HANDLING OF SENSITIVE INFORMATION

What it is

Confidential and sensitive information needs to be handled with care, including when it is circulated among IAM staff or shared with IAM members, experts, or anyone else associated with the IAM case in question.[99] One Action to consider is putting into place secure information management systems and protocols to ensure safe handling of sensitive information.

94 - Ibid.

95 - Ibid.

96 - Ibid., pg. 23.

97 - Ibid., pg. 24.

98 - Ibid., pg. 23.

99 - UN Office of the High Commissioner for Human Rights, 2015. Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law, pg. 80.

Why it is important
Inappropriate access to sensitive information can lead to an identification of the people with whom mechanisms have interacted.

SUGGESTED TOOLS

TOOL 1: Develop internal staff guidance on safe recording, storing, and handling of sensitive information

To ensure that all staff and external consultants are aware of the risks related to handling sensitive information, IAMs may consider developing internal staff guidance, such as that of the UN Office of the High Commissioner for Human Rights,[100] which, in summary, suggests the following points:

- The choice of equipment to record information (notebooks, computers, digital cameras, or audio and video recorders) should be based on methods that ensure the highest level of security given the overall context.
- The use of standardized codes for internal identification of victims, witnesses, or sources should be employed to ensure that identity and personal details of interviewees are protected.
- Cameras and audio or video recorders should be used only with the express consent of interviewees, and in situations where they do not present additional security concerns.
- All confidential and sensitive information should be securely stored, preferably in encrypted format, on a shared drive or another secure system.
- When disposing of computer equipment, information on computers should be properly deleted with the support of IT staff, as merely deleting files may not be enough to prevent recovery of confidential information.
- Notebooks should always be securely stored and not left unattended on top of office desks or inside vehicles.
- At the end of interviews, interpreters should hand over all their notes to IAM staff, and these notes should be destroyed at the first opportunity.
- After typing up interview notes, they should be shredded or burned. Similarly, photographs or audio and video recordings should be transferred to a secure encrypted storage system as soon as possible and the originals erased.
- If hard copies are kept, these should be stored in lockable filing cabinets and access restricted to those IAM staff who need to use them. For additional security, the filing system for documents should not be displayed on the outside of drawers.
- Security safeguards, such as passwords or encryption, should be used to protect all confidential and sensitive information on computers, including personal computers, if these are used for remote work.
- Confidential or sensitive information should never be exchanged over mobile phones; internal IAM phone extensions or password-protected e-mails should be used instead.
- Sensitive information should not be shared through free, open wireless networks such as those offered in hotels, airports, or other transport hubs because these can easily be tapped by external parties.[101]
- Confidential and sensitive information should not be perused in public places, such as restaurants or airports.

100 - UN Office of the High Commissioner for Human Rights - Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons

101 - Ibid., pg. 26. See also Tactical Technology Collective, 2016. Holistic Security – Trainer's Manual.

TOOL 2: Use standardized codes for internal identification of requesters, complainants and other cooperating persons at risk

Safe storage and handling of sensitive information requires that internal notes conceal or delete any information that could identify the persons who have provided information.[102] Guidance by the UN Office of the High Commissioner for Human Rights suggests that identity and personal details of interviewees should be protected and kept separately from the interview reports and other case-related information.[103]

The standardized use of codes for identifying requesters, complainants, and other cooperating persons is an important means of achieving this purpose.[104] For example, if the information provided by a specific source is recorded in a notebook, the personal data of the interviewee should be recorded on a separate sheet of paper and a code (such as V1) assigned for the person. This code would then appear at the beginning of the information recorded in the notebook.[105] If using an audio recorder, the name of the interviewee and his or her personal details would also best be registered separately and in code so that no connection can be made between the recording and the interviewee.

TOOL 3: Establish secure information management systems

Secure information management systems, with controlled access, could be set up to store, manage, and protect confidential and sensitive information, and allow access only to staff who require such information for their work.[106]

Password-protected and encrypted web-based platforms, with a shared space to register and access documents, have been a preferred choice of international human rights mechanisms that handle sensitive information.[107]

> ***Example***
>
> The Project Complaint Mechanism (PCM) of the European Bank for Reconstruction and Development has recently established secure web-based platforms for sharing information with external consultant working on a given case, and where access to sensitive documents can be controlled by the mechanism.

TOOL 4: Abstain from the use of photography in case-related documents and public reports

Considering the sensitive nature of the mechanisms' work and the high-stake cases they are often involved in, IAMs could consider not using photos of persons involved in complaints or of individuals facilitating the IAM process in any public reporting, including web-content, or outreach material.

IAMs' use of photos of requesters, complainants, and other cooperating persons (such as interpreters) in public reports can pose significant risks of reprisals to individuals who appear in pictures. Risk context is dynamic and subject to constant change. IAMs therefore need to carefully weigh the value and importance of using photos in their public reporting against possible risks of future reprisal against person(s) appearing in the images.

102 - UN Office of the High Commissioner for Human Rights, 2015. Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law, pg. 80.

103 - UN Office of the High Commissioner for Human Rights: Manual on Human Rights Monitoring, Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, pg. 25.

104 - Ibid.

105 - Ibid.

106 - UN Office of the High Commissioner for Human Rights, 2015. Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law, pg. 79.

107 - Ibid., pg. 70.

For the purposes of public reports, generic illustrations could be considered as an Action to replace photos. If photographs are considered necessary to demonstrate harm, guidance by the UN Office of the High Commissioner for Human Rights suggests that IAMs are advised to:

- Abstain from using photos or any other images that may disclose the identity or the place of residence of the person(s) involved in the case, participating in the IAM outreach event, or facilitating the IAM process.

- Assess, in all cases, potential implications of publicly disclosing information to a third party, even when consent of the subjects has been obtained.

- Consider whether the person(s) facing high levels of threat wish to be photographed or filmed as a means of self-protection and assess the risks of following such a strategy.

- Not disclosing photos if there is a risk of harm, of if the level of risk cannot be ascertained.[108] Guidelines developed by the Inspection Panel and the Compliance Advisor Ombudsman both highlight the risks of publicly using photos that can lead to identification of individuals.

The Inspection Panel's reprisals guidelines note that when documenting aspects of its work through photographs, "the Panel will not utilize images of individuals at risk of indications of their locations. The Panel seeks the consent of all individuals that may be identifiable in their photographs after providing information about how the photographs may be used."[109]

The guidelines of the Compliance Advisor Ombudsman also note that the mechanism will not "take photographs of individuals involved in a complaint without their express consent" and that it will not "use identifiable images of individuals with confidentiality protection, or indications of their locations, in documenting aspects of its work through photographs, without their express consent" for doing so. Photographs of parties involved in a CAO case will only be used for publication purposes when appropriate permissions have been sought and the parties are aware of how the images will be used.[110]

108 - Office of the UN High Commissioner for Human Rights, 2015. Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law.

109 - Inspection Panel, Guidelines to Reduce Retaliation Risks and Respond to Retaliation During the Panel Process. http://inspectionpanel.org/sites/ip-ms8.extcc.com/files/documents/IPN%20Retaliation%20Guidelines_2018.pdf

110 - Compliance Advisor Ombudsman, CAO Approach to Responding to Concerns of Threats and Incidents of Reprisals in CAO Operations, http://www.cao-ombudsman.org/documents/CAO-Reprisals-web.pdf

PHOTO: MICI

BUILDING THE CAPACITY OF IAMs

The best protection IAMs can provide to cooperating persons is to be aware of potential risks of harm and to exercise good judgement, caution, and sensitivity toward these risks in all interactions. A limited understanding of the operational risk context of a given case and lack of care and negligent behavior of IAM members/staff/consultants can put requesters, complainants, and other cooperating persons at risk of harm.

The limited capacity of IAM staff to assess and address risks of reprisal has been raised by all interlocutors, including IAM staff, as one of the major challenges to more effectively prevent and respond to reprisals.

There are several Actions IAMs can consider to build staff capacity to better assess and address risks of reprisals, including:

- Adopting public policy and internal guidance
- Providing regular staff training
- Building alliances with external resource organizations
- Ensuring an institutional memory of reprisals
- Appointing IAM focal points on reprisals

ACTION 19: ADOPT PUBLIC POLICY ON REPRISALS AND DEVELOPING INTERNAL STAFF GUIDANCE

What it is

A public policy on reprisals codifies an IAM's intentions and approaches to systematically assess and address the risks of reprisals, as well as its capacity to do so. It could exist with complementary internal staff guidance about implementing the policy.

Why it is important

Adopting a public policy statement serves three important purposes. First, it communicates that the IAM takes risks of reprisals seriously. Second, it clarifies that IAMs will act in response to risks in each case. Third, it affirms that IAMs will ensure that staff have the necessary capacity to do so.

Examples

At present, two members of IAM Network have adopted public statements (guidelines) on preventing and addressing reprisals (the World Bank Group's Inspection Panel in 2016 and the Compliance Advisor Ombudsman in 2017). An additional three IAMs have started the process to develop their own guidelines (the Independent Consultation and Investigation Mechanism of the Inter-American Development Bank, the Complaints Mechanism of the Asian Development Bank, and the Independent Review Mechanism of the Green Climate Fund).

Among the mechanisms that have adopted a public policy statement on reprisals, the Compliance Advisor Ombudsman has noted that it is in the process of developing more detailed guidance to its staff.

SUGGESTED TOOLS

TOOL 1: Template for a public policy concerning reprisals

Based on the practice of human rights mechanisms of the United Nations,[111] IAMs could consider reflecting the following in their public policy statements:

Objectives and guiding principles

- Establish a zero-tolerance policy for any form of reprisal against requesters and other related stakeholders for having cooperated with the IAM, setting clear expectations that no reprisals should occur before, during, or after the IAM process.

- Define, in broad terms, acts that can be considered reprisals. A definition can rely on illustrative examples (such as the different forms of reprisal observed by IAMs). However, as reprisals can vary greatly depending on context, it should note that examples are illustrative, not exhaustive. Acts of reprisals should not be narrowly defined to cover only the most serious forms of retaliation, but also include intimidation and verbal harassment. In line with the approach currently employed by UN Human Rights Mechanisms, reprisals could be defined to include intimidation, threats, harassment, punishment, judicial proceedings, use of violence, murder or other retaliatory acts against requesters and others associated with them or with the IAM process.

- Given that it may be challenging to identify the direct cause of a reprisal, the IAM could act to prevent reprisals and respond to allegations of reprisals even when the link to the IAM process is unclear or when the source of the threat suggests that the reprisal is not related to the IAM case.

- Highlight that the IAM considers protection of requesters and others associated with them or with the IAM process to be the shared responsibility of:

  > The State concerned by the IAM process (whether during problem solving, compliance review, or outreach)

  > The IAM's parent institution

  > The IAM

  > The direct parties to the process, including the project implementing agency and associated business relationships

  > The requesters and others related to them

  > Others who can positively or negatively influence the safety of those at risk of reprisal, and indirectly or directly strengthen their protection.[112]

- Establish that the IAM expects that all parties take the necessary measures to reduce risks of reprisals (and address reprisals where these occur), and that the IAM will engage with these parties, to the greatest extent possible, to mitigate any risks.

- Establish that the policy will be implemented in line with the principles of participation, informed consent, and do-no-harm – that is, in a manner that does not jeopardize the life, safety, freedom, and well-being of the person(s) concerned – and that any measures to reduce risks of reprisal and address instances of reprisal will be discussed and agreed with the persons concerned.

- Provide examples of measures that the IAM can take to reduce risks of reprisals and

111 - See Guidelines against intimidation or reprisals adopted at the twenty-seventh meeting of chairpersons of the human rights treaty bodies (San Jose Guidelines). UNs Doc. HRI/MC/2015/6 and the Special Procedures of the UN Human Rights Council: Enhanced Response to Acts of Intimidation and Reprisal for Cooperation with the Special Procedures http://www.ohchr.org/EN/HRBodies/SP/Pages/Actsofintimidationandreprisal.aspx

112 - See Office of the UN High Commissioner for Human Rights: Manual on Human Rights Monitoring. Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons, pgs. 5–6, for a discussion on the shared responsibility to protect.

address reprisals and note that these measures and additional steps that can be taken will be elaborated in internal policy documents not publicly shared to guarantee the safety of the person(s) concerned and those who may benefit from the measures in the future.

- Communicate that the policy document (and related internal staff guidance) will be revised on an ongoing basis, and invite individuals, groups, and organizations to submit feedback on the policy statement and its effectiveness to inform such revisions.

Applicability, scope, and limitations

- Note that persons cooperating with the IAM – requesters, complainants and those associated with them (including family and friends, and individuals or organizations facilitating their interaction with the mechanisms) or with the process (including IAM staff, consultants, interpreters, drivers, expert witnesses) – may be victims of reprisals, and that policy statement and associated measures will seek to prevent and address all cases of reprisals against them.

- Establish that the policy applies to all activities of the IAM and to all its processes and functions, including pre-eligibility, eligibility, problem solving, compliance review, monitoring, and outreach activities.

- Provide clarity on who is expected to adhere to the policy. At a minimum, this should include IAM members, staff, experts, consultants, and others who facilitate an IAM process.

- Appoint and refer to a focal point on reprisals in each IAM.

- Be transparent about the IAM's limitations to protect requesters and associated persons so that people do not take risks in a false sense of security that the IAM can protect them. Note, for example, that the mechanism is not an enforcement agency and cannot provide physical protection to the persons concerned or otherwise guarantee that reprisals will not ensure because of the process.

Measures to prevent reprisals

- Note that the reprisals policy will be shared with all parties to the IAM process at its earliest stages in an accessible format.

- Establish that the IAM will proactively seek information from requesters and other cooperating persons about perceived risks of reprisal (or reprisals that have occurred), and that this discussion will become routine for all requests, at the earliest stages of the process.

- Commit to conducting a participatory risk assessment (defined as the possibility of events that result in harm) of reprisal at the earliest stage possible and agree with those concerned on measures to be taken to reduce risks based on this assessment. Commit to regularly reviewing the assessment and revising the agreed measures at each stage of the process, and when circumstances so warrant.

- Establish that in instances in which the IAM concludes that serious reprisals are possible, the mechanism will decide, together with those concerned, whether to proceed with the case at all, or whether to postpone or fast-track the registration and process.

- Note that the IAM will work to strengthen working relationships with actors that can positively influence the safety of those at risk and indirectly or directly strengthen their protection, including human rights mechanism and nongovernmental organizations with expertise in protection strategies for human rights defenders.

Addressing allegations of reprisals

- Highlight that all allegations of reprisals will be assessed by the IAMs as a matter of priority and determine the most appropriate courses of action, considering the responses that have been agreed with the person(s) concerned.

- Ensure that where circumstances so warrant, IAMs will respond with immediate action before verifying allegations. If the person concerned is in immediate danger, IAMs will focus their efforts on reducing the source of the threat, including alerting senior management and the Executive Board of their parent institution, as appropriate and where this will not create further risks. All responses will be considered with the consent of the persons concerned, and in line with the principle of do no harm.

- Highlight that after having identified the best courses of action, the IAM will develop a protection timeline with the person(s) concerned or, where direct engagement with him/her/them is not possible, with their representatives. The timeline will establish how the actions will be put into practice, by whom and when. IAMs will work closely with the person(s) at risk and relevant partners to implement the agreed measures, and will do so through regular communication, review, and follow-up.

- Note that in addition to engaging with senior management and the Executive Board(s) of the parent institutions, IAMs may seek the support of other external actors that can provide further support to ensure the protection of the person(s) at risk.

- Note that, regardless of the status of the IAM process (active or closed), the IAM will consider the matter active until it has been verified by the person(s) concerned that this is no longer the case or, if that is not feasible, seek other alternatives for follow up.

- Emphasize that all instances of reprisal will be included in any case-related documentation, where it is considered that doing so will not further jeopardize the security of the persons concerned. IAMs may also wish to note that their annual reports will include disaggregated data on reprisals.

TOOL 2: Develop complementary internal guidance

In their public policy statement, IAMs may wish to include examples of preventative measures they can take to reduce risks.

However, to ensure that staff and others associated with the IAM process are fully informed of the measures they can take to assess and reduce risks, and respond to reprisals should these occur, it is recommended that IAMs prepare additional internal guidance documents. It is advised that IAMs do not make such documents public, as requesters and other related stakeholders can be put at further risk if the measures become known to the source of the threats. In line with the measures suggested in this toolkit, internal guidance documents could cover:

- Templates, guiding questions, and sources of information for reprisals risk assessments

- Resource organizations and human rights mechanisms that can support implementation of measures to reduce risks and respond to reprisals and how to solicit this support

- Protocols for safe communication and safe information management systems

- Field codes of conduct to ensure confidentiality of requesters, complainants, and other cooperating persons in the context of field visits.

ACTION 20: PROVIDE REGULAR STAFF TRAINING

What it is

IAMs may consider establishing regular training for their members and staff on how best to identify and address risks of reprisals and respond to reprisals that have occurred.

Why it is important

Regular staff training is essential to ensure that all IAM members and staff have the same level of knowledge and skills to assess and address reprisals, and to ensure ongoing skill development.

Learning how to assess and address risks of reprisal cannot be captured in one training session – understanding risk is a way of thinking that requires ongoing training and skills development. Although one-off training may be provided to new employees and consultants, it is important that training schemes are put in place for continuous skills development. To retain knowledge, skills need to be practiced and refreshed on a regular basis. With regular training, IAMs can more easily identify any skill gaps within the existing workforce. By identifying these gaps early on, staff can be trained at the required areas so that they can fulfil their roles effectively.

Example

Among members of the IAM Network, the Compliance Advisor Ombudsman (CAO) has taken the lead in working with expert organizations to build staff capacity to assess and address risks of reprisal.

In 2017, CAO invited the organization Front Line Defenders to train CAO staff in how to reduce risks of reprisals related to the CAO process. This training, which included case studies that reflected the operational context of the mechanism, served as an important means to map Actions available to them to address risks and respond to reprisals.

SUGGESTED TOOLS

TOOL 1: Include reprisals risk training in mandatory induction programs and skills development plans

An important means to ensure all IAM staff have the same baseline knowledge of risks of, and measures to address, reprisals is to include reprisals risk training as part of the mandatory induction programs for new staff. This also sets the expectation clearly for new staff that addressing reprisals in IAM activities is a crucial component of their work.

However, training is a process and requires sufficient time to achieve full impacts. To ensure staff benefit from regular training sessions that reflect the changing (reprisals) realities of the IAMs, the mechanisms may also wish to consider reflecting reprisals-related skills development as a key feature of staff job descriptions and skills development plans.

TOOL 2: Work with expert organizations to design and deliver staff training

Working with expert resource organizations is key, as IAMs do not currently have the expertise themselves on how to best work with individuals and groups at risk (of reprisal).

ACTION 21: BUILD ALLIANCES WITH EXPERT ORGANIZATIONS

What it is

IAMs could consider how to foster an ongoing working relationship with organizations specialized in working with individuals and groups at risk.

Why it is important

Building alliances with expert resource organizations can provide support needed to reduce risks of reprisals and response options.

Suggested tools

TOOL 1: Compile a list of useful organizations, by theme or region

IAMs are encouraged to compile a list of expert organizations and mechanisms that can:

- Serve as important sources of information for risk assessments
- Function as external expertise that can be brought in to support IAM reprisals risk assessment in high-stake and high-risk cases
- Build the capacity of IAM staff to assess and address risk of reprisals

- Act as facilitators in IAM processes, such as intermediaries where direct IAM contact with requesters/complainants may significantly jeopardize their security and well-being

- Support the implementation of preventative measures where risks of reprisal are high

- Support IAMs in responding to reprisals where these have occurred.

The list of suggested resource organizations, included in the appendixes, can be a useful starting point for such a list.

TOOL 2: Include representatives of expert organizations in IAM advisory groups or as rostered experts

Some IAMs have established external advisory groups that provide pro bono advice to the mechanisms.[113] These groups are an important means to ensure continuous learning and improvement for mechanisms and their staff. IAMs are encouraged to include, as members of the advisory groups, representatives of reputable CSOs that work on human rights defenders and protection measures. Similarly, IAMs that rely on independent experts to assist with the review of complaints [114] could consider including individuals with similar expertise in their roster of experts. This will help build internal IAM capacity to assess and address risk of reprisals and open important channels of communication with external networks that can be triggered for additional protection measures when needed.

ACTION 22: DOCUMENT PAST EXPERIENCES

What it is

IAMs are encouraged to consider how they can create a process to systematically capture institutional knowledge about past instances of reprisals and measures taken to address them, to make this information accessible to people as they come into the organization.[115]

Why it is important

At present, none of the IAMs have a system in place to ensure a formal institutional memory of past situations and how they have been addressed. While some of the current institutional knowledge about reprisals has been placed into procedures and policies, most is still in the heads, and hands, of individual managers and experts who have worked with the mechanisms on cases for which reprisals have been observed.

The principal reason for keeping records is to retain an institutional memory of past instances of reprisals, the actions taken to respond to such instances, and their effectiveness.[116] Keeping track is also important to remind those involved about what has been agreed, and to advise new staff and consultants who may be brought in to support problem solving or compliance reviews that have already commenced.

Keeping a systematic record can also be used to justify measures to respond to reprisals based on past good practice. This will help IAMs effectively engage with management and decision-makers of parent institutions, which, similar to IAMs

113 - See, for example, the External Consultative Group of the Independent Consultation and Investigation Mechanism of the Inter-American Development Bank (MICI) (http://www.iadb.org/en/mici/external-consultative-group,20947.html).

114 - See, for example, the Roster of experts of the Project Complaints Mechanism of the European Bank of Reconstruction and Development (current membership at http://www.ebrd.com/work-with-us/project-finance/project-complaint-mechanism/pcm-experts.html).

115 - Ashkenash, 2013. "How to Preserve Institutional Memory," Harvard Business Review (March 5).

116 - The establishment of a comprehensive record of information on all alleged instances of intimidation and reprisals is one of the key measures suggested by the UN Human Rights Treaty Bodies and the Special Mandate Holders of the Human Rights Council (also known as Special Rapporteurs) in their responses to reprisals.

themselves, experience high staff turnover. New parent institution staff and Board members are likely to be more accepting of suggested measures that require their action if these measures can be justified based on past good practices.

Logging threats and other reprisals will also inform reprisal risk assessments. For example, if the log reports security incidents around periods before elections, it is likely they will occur again at the following pre-electoral period. [117]

Examples

The Special Procedures of the UN Human Rights Council – known as UN Special Rapporteurs or Working Groups – agreed, in June 2015, to keep a comprehensive record of all cases of intimidation and reprisals against individuals and groups cooperating with them to ensure an overview of reported reprisals and actions taken to address them.

Similarly, reprisals guidelines adopted by the UN Human Rights Treaty Bodies foresee the establishment of a comprehensive record of information on all alleged instances of intimidation and reprisals

(Guidelines against intimidation or reprisals adopted at the twenty-seventh meeting of chairpersons of the human rights treaty bodies (San Jose Guidelines). UN Doc. HRI/MC/2015/6.)

SUGGESTED TOOLS

TOOL 1: Develop an explicit strategy for how to maintain institutional knowledge

IAMs may consider developing a strategy for how to maintain institutional knowledge about reprisals. As part of his strategy, IAMs can identify key issues that every staff member should know and be able to do, based on past instances of reprisals and responses – whether successful or unsuccessful.

TOOL 2: Use technology to create a platform for curating institutional knowledge

The selection (or redefinition) of a technological platform is an important tool to consider so as to ensure that staff continually captures and curates institutional knowledge about reprisals.

The Pan American Health Organization and the World Health Organization, while not specifically working with sensitive information, have relied on DSpace (knowledge sharing plattform) to maintain institutional knowledge, based on the fact that it is:

- A free and open code tool and one of the largest communities of users and developers worldwide
- May be adapted for integration with other platforms/databases
- Guarantees that digital resources are preserved in the platform itself
- Allows restricting the use of a document, collection, or virtual community to a person or group of users with permission to have access to this(these) resource(s)
- Can be used to define different roles, work groups, and permission levels of the flow of information for contributing to the platform
- Can be modified according to the needs and requirements of the institution; it allows all type of digital content, text, images and videos to be recorded and preserved; it is easy to install, and a wealth of support documentation is available on the internet
- Offers the possibility of customizing the statistics module as an analysis input for decision-making.[118]

117 - Eguren and Caraj, 2009. New Protection Manual for Human Rights Defenders (Protection International), pg. 50

118 - Pan American Health Organization/- World Health Organization, 2015. Methodologies for Information Sharing and Knowledge Management in Health How to Organize and Preserve the Institutional Memory, pgs. 4–5.

IAMs can also consider working with Intel's internal wiki (called Intelpedia), which gives staff a way of both capturing and accessing important terms, procedures, and other information such as historical incidents.

IAMs can also rely on their current information management systems, to the extent these can guarantee that sensitive information cannot be accessed by persons without access rights.

TOOL 3: Work with expert organizations to ensure the safety of the preferred management system

To ensure the digital security of the preferred information management system, IAMs may wish to consider working with the IT teams of their parent institutions or with external resource organizations specialized in sensitive information.

ACTION 23: APPOINT IAM FOCAL POINTS ON REPRISALS

What it is
Each IAM can consider appointing an internal focal point on reprisals to coordinate the mechanism's work relating to reprisals.

Why it is important
Appointing a senior focal point within each IAM is an important signal that the mechanism takes the matter of reprisals seriously. Appointing a focal point on reprisals and communicating this appointment publicly – for instance, as part of the reprisals guidelines – also makes it easier for management of the IAM's parent institution, victims of reprisals, or organizations supporting them to know to whom to turn for reporting instances of reprisals.

A focal point typically also represents the mechanism at external meetings relating to reprisals, including with expert resource organizations or with other members of the IAM Network. In this regard, he/she also serves an important role as the resource person on reprisals who, when needed, can advise other staff on available measures to assess and address risks, and respond to alleged reprisals.

Examples

The Inspection Panel, in its guidelines to reduce retaliation risks, appointed the Panel's Executive Secretary as the overall focal point to coordinate its work preventing and responding to allegations of retaliation, while noting that each assigned case officer will continue to act as the focal point for the case at hand.

Among the UN human rights mechanisms, the Treaty Bodies, in 2015, also established a system of appointment by each treaty body of at least one of its members as a rapporteur or focal point on intimidation or reprisals to receive and assess information on alleged intimidation and reprisals and report to his/her respective treaty body on measures taken to address allegations. Among the treaty bodies, the Sub-Committee on Torture, in line with its mandate to visit countries, further elaborated that its focal point will ensure that any additional information discovered concerning reprisals is reflected in the visit report.

The UN Special Procedures have also followed suit: in line with their coherent framework for action to prevent and address intimidation and reprisals Special Procedures were decided to appoint a focal point on reprisals among its members on an annual basis to coordinate the collective work of the mechanisms on reprisals.

See Acts of intimidation and reprisal for cooperation with the special procedures: https://www.ohchr.org/EN/HRBodies/SP/Pages/Actsofintimidationandreprisal.aspx

WORKING WITH PARENT INSTITUTIONS TO ENHANCE AWARENESS OF AND RESPONSIVENESS

ACTION 24: RAISE AWARENESS AMONG MANAGEMENT AND DECISION-MAKERS

What it is

A key preventative measure is to systematically work to enhance awareness of management and decision-makers of parent institutions about risks of reprisals that requesters and other related stakeholders may be exposed to, and the need to address these risks in project design and implementation.

Why it is important

IAMs have limited leverage over potential sources of reprisal and are largely dependent on parent institutions to effectively prevent and address reprisals. IAMs have indicated that limited awareness among management and decision-makers of their parent institutions about the risks of reprisal is a major concern. Limited awareness poses several challenges for IAMs to effectively prevent and address reprisals, including:

- Limited recognition of the respective responsibilities of the parent institutions and IAMs to prevent reprisals in the context of IAM processes or outreach activities
- Few or no upfront requirements on borrowers/fund recipients/clients to help ensure that no reprisals take place during project design and implementation and in the event of an IAM intervention
- Reluctance to support implementation of preventative measures that have been agreed as necessary between IAMs and requesters and associated persons to reduce risks of reprisal and address reprisals if it occurs
- Limited willingness and capacity to engage with reprisals once they occur.

SUGGESTED TOOLS

TOOL 1: Invite an authoritative voice on reprisals for an informal dialogue with the Board

The risk and dangers of reprisals is a topic rarely discussed by the Executive Boards of IAMs' parent institutions. Limited space for this type of discussion makes it challenging for IAMs to raise the issue when requiring support from the Boards.

One way to address the issue could be by organizing an informal discussion with the Board outside of a formal room meeting. IAMs may consider inviting the recently appointed Senior Official on UN Systemwide Efforts to address reprisals against individuals and groups that seek to cooperate with the UN. As an authoritative, balanced, and constructive interlocutor, an informal working lunch with the senior official could foster interest on the part of the Boards on the issue of reprisals. IAMs could consider relying on the good offices of the UN Office of the High Commissioner on Human Rights to organize a meeting of this kind.

Example

In recognition of the limited space for discussions at the Board level, the UN Office of the High Commissioner for Human Rights facilitated a "Dean's lunch" with the UN Office of the High Commissioner for Human Rights and the Executive Directors of the World Bank's Board in the context of the recent Bank's review of its environmental and

social Safeguard Policies. This lunch, hosted by the Dean of the Board, provided an important opportunity for an informal and inclusive discussion on the role of human rights in the proposed Safeguards framework, and generated a high-level interest among Directors.

TOOL 2: Share IAM reprisals policies/guidelines with the Boards and senior management of IAMs' parent institutions

Discussions with Board Members at the World Bank Group suggest that while there is growing concern at the Boards about the globally deteriorating situation for civil society and increase in reported reprisals, Boards of Executive Directors are not aware of IAMs' efforts to address this matter and none have heard about the adoption of reprisals guidelines by the mechanisms.

To enhance awareness on the part of the Boards and senior management of parent institutions, IAMs that have adopted reprisals guidelines may wish to consider circulating these to Boards and senior management. Realizing that Directors often change, IAMs might consider circulating reprisals information jointly with general information provided about the mechanism to new Directors. In addition, IAMs could attach reprisals guidelines to all case-related information that is shared with them.

TOOL 3: Record reprisals in case-related reports

Reflecting reprisals in case-related reporting in a more systematic manner can serve as an important action to raise awareness among parent institution management about risks of reprisals, as it encourages them to consider addressing reprisals in their action plans and related supervisory missions. Systematically reporting reprisals has also been noted to have an important deterrent effect for future reprisals.

IAMs can consider including any instances of reprisals in case-related reports (such as eligibility decisions, problem-solving, compliance review, and monitoring reports). Doing so, however, should not further jeopardize the security of the victims of reprisal and should only be done with the express consent of those concerned. In accordance with the principle of do no harm, case-related reprisals risk assessments should consider the extent to which publicly reporting reprisals can pose further risks to the safety and well-being of the individuals or groups concerned. When risks are considered too high, or IAMs lack sufficient information to assess the level of risk, those cases should not be included in reports.

Examples

In the context of the UN Secretary General's reporting mandate on reprisals, the practice to name individual countries that have retaliated or condoned acts of reprisal against persons who have cooperated with the UN has had an important deterrent effect. Systematically reporting reprisals in the context of IAM activities will not eliminate future risks of reprisals, but will increase the perceived cost of retaliating, and thus lower the probability of reprisals.

Reporting reprisals in case-related documents is currently done by two of the members of the IAM Network: the Inspection Panel and the Compliance Advisor Ombudsman.

In the case of the Inspection Panel, its guidelines on preventing reprisals (2016) highlight that the Panel will "mention all instances of threats, intimidation or other retaliation in its eligibility and investigation reports, while respecting the confidentiality of complainants and interviewees, unless those affected request the Panel not to do so."

The Compliance Advisor Ombudsman, in keeping with its recently released approach to address reprisals (2017), has also committed to reflecting "any significant security concerns or incidents in case-related CAO reports as appropriate, with the concerned person or group's consent and where it is safe for the concerned person or group to do so."

TOOL 4: Include aggregate data on reprisals in annual reports/preparing stand-alone reports on reprisals in the IAM context

To enhance awareness of management and decision-makers of IAMs' parent institutions about reprisals, IAMs may also wish to include aggregate information on reprisals in their annual reports.

Drawing lessons from their caseloads, IAMs with an advisory function may also consider doing stand-alone reports on the totality of instances of reprisals in their operations.

Example

The recently released Approach of the Compliance Advisor Ombudsman to preventing and responding to reprisals notes that CAO, in its annual reports, will include aggregate information on threats and reprisals, drawing on information received in the course of its work as the independent recourse and accountability mechanism for IFC and MIGA.

TOOL 5: Lobby for the appointment of an institutional leadership group/ senior advisor on reprisals

IAMs may wish to consider proposing the appointment of a focal point on reprisals within the parent institution. This leadership group/senior advisor could support the IAM's efforts to respond to reprisals and be accountable for the institution's response.

Establishing an institutional focal point will also help IAMs have better established lines of communication with parent institution management on measures needed to avoid and address reprisals, whether on a case-by-case or institutional level. IAMs may wish to initiate discussions with parent institution management about the appointment of such a focal point.

Examples

The Secretary-General of the United Nations appointed Assistant Secretary General Andrew Gilmour to receive, consider, and respond to allegations of intimidation and reprisals against human rights defenders and other civil society actors engaging with the UN. While the mandates of the UN and its human rights mechanisms are not comparable to that of IAMs' parent institutions, the appointment of a senior UN representative is interesting as it reflects that the United Nations has been struggling with same problems of reprisals as IAMs and their institutions, and has, after years of sustained pressure from civil society, now started coordinating a more systematic response. Information about reprisals can be shared here:

https://www.ohchr.org/EN/Issues/Reprisals/Pages/HowToShareInformationAboutCases.aspx and through email via reprisals@ohchr.org

At the World Bank, the appointment of a Leadership Group on Sexual Orientation and Gender Identity (SOGI) in 2016 sets an important precedent for how the World Bank has navigated a politically sensitive subject. The World Bank's Leadership Group was appointed following the adoption of the revised Safeguards framework in 2016, in which LGBTI (lesbian, gay, bisexual, transgender, and intersex) issues became highly politicized. In 2016, the President of the World Bank created a new senior position responsible for promoting lesbian, gay, bisexual, transgender, and intersex inclusion throughout the work of the World Bank.

ACTION 25: ENCOURAGE PARENT INSTITUTION MANAGEMENT TO ESTABLISH A ZERO-TOLERANCE POLICY REGARDING REPRISALS AND MEASURES TO IMPLEMENT POLICY

What it is

A recurring concern among both IAMs and civil society organizations is the limited extent to which IAMs' parent institutions communicate the expectation to their borrowers/fund recipients/clients that reprisals and other forms of repression will not be tolerated. IAMs could therefore consider how to encourage parent institutions to better communicate this expectation.

Why it is important

The absence of upfront requirements on borrowers/fund recipients/clients to abstain from reprisals has made it challenging for parent institutions and their accountability mechanisms to prevent reprisals in a systematic manner, and it significantly reduces the leverage the parent institution can realistically exercise over the former should allegations of reprisals become an issue.

Integrating this requirement could help establish clear roles and responsibilities for prevention, mitigation, and remedy of any potential reprisals, as well as facilitate cooperation and effective management of issues as they arise throughout the project's life cycle.

TOOL 1: Parent institution zero-tolerance policy and related reprisals guidance

IAMs can consider encouraging parent institutions to adopt a zero-tolerance policy that also commits the institution to assessing and adopting measures to address retaliation risks. The project's initial environmental and social impact assessment could, as a matter of good practice, direct specific attention to the environment for public participation in the country concerned, and provide an understanding of the extent to which State authorities and other relevant entities demonstrate, in law and in practice, the capacity and commitment to protect individuals and groups against reprisals. This layer of the assessment could include the state of civil society, the situation of human rights defenders, instances of previous reprisals, and State authorities' responses to earlier instances of reprisals. Consultation processes that inform the development of this impact assessment and project design should ensure that all potentially affected individuals and communities are consulted, their views robustly considered, and their consent obtained (when required or useful). Measures in response to retaliation risks should be included in project design and implementation. This assessment should be robust enough to inform a later retaliation risk assessment by the IAMs.

Additionally, IAMs can consider suggesting to Management that their parent institutions develop their own guidelines for parent institution staff on how to assess and address risks of reprisals. This kind of guidance has been raised by interviewees to this toolkit as particularly important for country-level staff, whose interaction with project implementing agencies and borrowers both before and in the context of IAM interventions has come under critique by civil society organizations as posing risks to the confidentiality and well-being of requesters and other related stakeholders. Examples include engaging with requesters, thereby making their identities known, at an early stage of the process in a well-intentioned effort to resolve the problem. In this regard, it has been noted that parent institution management would stand to benefit from the kind of guidance that several of the IAMs have developed to address risks of reprisals.

IAMs could encourage their parent institutions to build on their existing good guidance notes to reflect risks of reprisals.

Examples

In the context of the adoption of its Approach to reprisals, CAO has committed to seeking to support efforts of its parent institutions (IFC and MIGA) to develop their own operational response to the issue of threats and reprisals. IFC has adopted a statement indicating zero tolerance related to retaliation:

https://www.ifc.org/wps/wcm/connect/ec379db4-56f1-41e1-9d86-8ea05945bc67/201810_IFC-position-statement-on-retaliation-and-threats-of-reprisals.pdf?MOD=AJPERES.

Among the IAMs' parent institutions, the IDB appears to have included some references to risks of reprisal in internal "good practice" guidance on stakeholder engagement, in particular with regard to the accessibility of grievance mechanisms and in its recent publication on Social Impact Assessment.

The EBRD is, for its part, in the process of developing an internal guidance notes for staff and management on how to best handle allegations of human rights abuses, including reprisals, in the context of EBRD-funded projects.

TOOL 2: Include a reprisals requirement in loan agreements with borrowers and placing borrowers that retaliate on exclusion lists

Introducing a standard clause on reprisals in contracts between the IAMs' parent institutions and borrowers/fund recipients/clients could be an important way to put the latter on notice that reprisals will not be accepted. Introducing a reprisals clause could also serve as an important opportunity for parent institutions to create a dialogue with its borrowers/fund recipients/clients regarding these terms of the contract, the expectations and challenges they raise, and how they can best be met.

A standard "reprisals clause" could specify that the institution expects that the borrower/fund recipient/clients will take measures to prevent reprisals, and that reprisals against individuals or groups expressing concerns about projects/activities supported by the parent institutions projects, or that cooperate with the parent institution's accountability mechanisms, could lead to a termination of the contract, as breaches of other clauses would.

It is worth noting that several of the major multilateral development banks have issued, as an integral part of their environmental and social safeguard policies or stand-alone frameworks, a zero-tolerance approach to fraud, corruption, collusion, coercion, obstruction, money laundering, and terrorist financing in relation to their activities and projects. Borrowers/fund recipients/clients that do meet these expectations are put on exclusion lists. IAMs can therefore also consider lobbying for inclusion of reprisals on their parent institutions' exclusion lists.

As for contractual obligations, a growing number of international trade agreements and supply chain contracts prepared by multinational businesses impose such standards in the human rights area of labor rights. By way of illustration, the Coca-Cola company communicates clearly that it expects all its suppliers and system partners to embrace responsible workplace practices and uphold the principles of the company's human rights policy. These expectations are communicated through Coca-Cola's Supplier Guiding Principles, which are part of all contractual agreements between Coca-Cola Company and its direct and authorized suppliers.[119]

119 - Coca-Cola: Suppliers and Customer Partnerships. (http://www.coca-colacompany.com/our-company/suppliers)

Examples

The African Development Bank, through its Whistle-blowing and Complaints Handling Policy, which covers whistle-blowers and complainants to the Bank's independent accountability mechanism, establishes zero tolerance against reprisals. It specifies that "retaliation shall not be permissible against any Whistleblower or Complainant. 'Retaliation' means any act of discrimination, reprisal, harassment, or vengeance, direct or indirect, recommended, threatened or taken against a Whistleblower or Complainant by any Person because the Whistleblower or Complainant has made a disclosure pursuant to this Policy.

A useful model for IAMs to consider is the preambular language in the foundational legal instrument of the European Bank for Reconstruction and Development. It notes that contracting parties are "[c]ommitted to the fundamental principles of multiparty democracy, the rule of law, respect for human rights and market economies." (Agreement establishing the European Bank for Reconstruction and Development)

The Norwegian Government's Pension Fund has also developed guidelines with criteria for the exclusion of companies from the fund´s investment universe, including those that are allegedly involved in serious human rights violations (see Box 3).

Box 3. Extract from the Government of Norway's "Guidelines for observation and exclusion from the Government Pension Global Fund"

Section 3. Criteria for conduct-based observation and exclusion of companies

Companies may be put under observation or be excluded if there is an unacceptable risk that the company contributes to or is responsible for:

a) serious or systematic human rights violations, such as murder, torture, deprivation of liberty, forced labor and the worst forms of child labor

b) serious violations of the rights of individuals in situations of war or conflict

c) severe environmental damage

d) acts or omissions that on an aggregate company level lead to unacceptable greenhouse gas emissions

e) gross corruption

f) other particularly serious violations of fundamental ethical norms.

Source: https://www.regjeringen.no/globalassets/upload/fin/statens-pensjonsfond/formelt-grunnlag/guidelines-for-observation-and-exclusion-from-the-gpfg---17.2.2017.pdf

APPENDIX 1. SOURCES OF INFORMATION

1. SUGGESTED SOURCES OF INFORMATION/ ORGANIZATIONS

The suggested sources of risk information are presented in alphabetical order and hyperlinked for ease of access.

African Commission on Human and Peoples' Rights (Special Rapporteur on Human Rights Defenders)
The African Commission on Human and People's Rights has a Special Rapporteur on human rights defenders, who has a mandate to seek, receive, examine, and act upon information on the situation of human rights defenders in Africa and, in this regard, submits reports at every ordinary session of the Commission. The current Special Rapporteur has been active in issuing press releases, including to reject acts of reprisal against human rights defenders who attempt to work with the Commission. These press releases could be consulted to map the risk context in member states of the African Union.

> http://www.achpr.org/mechanisms/human-rights-defenders/

Amnesty International
Amnesty International is a CSO that is independent of any political ideology, economic interest, or religion that works to address human rights across all regions. Its annual state of the world's human rights provides an important snapshot of the global and country-level trends. Amnesty's country-specific information and annual reports are a useful source of information for the IAM risk assessments. The organization also has individuals at risk unit that regularly provides country-specific information and reports about individuals at risk.

> https://www.amnesty.org/en/countries/

CIVICUS
World Alliance for Citizen Participation is an international alliance of members and partners that constitutes an influential network of organizations at the local, national, regional, and international levels, and spans the spectrum of civil society. The CIVICUS Monitor, with a global scope, provides an important source of country-specific information to assess the state of civil society.

> https://monitor.civicus.org/

Council of Europe Commissioner for Human Rights
The Commissioner for Human Rights is an independent and impartial nonjudicial institution established in 1999 by the Council of Europe to promote awareness of and respect for human rights in the 47 Council of Europe member states. The Commissioner conducts country visits and reports publicly on these visits. These reports contain conclusions and relevant recommendations to help address shortcomings, including with regards to States' treatment of human rights defenders.

> https://www.coe.int/en/web/commissioner/home

Frontline Defenders
Front Line Defenders was founded in Dublin in 2001 with the specific aim of protecting human rights

defenders at risk. The organization's reporting on individual cases and country situations is particularly useful for the IAM risk assessment.

> https://www.frontlinedefenders.org/

Human Rights Treaty Bodies of the United Nations

The ten UN human rights treaty bodies are 10- to 24-member expert committees that review countries' performance under their ratified international human rights treaties (http://www.ohchr.org/EN/HRBodies/Pages/HumanRightsBodies.aspx). Treaty bodies deal with issues such as civil and political rights (including freedom of association and participation rights), economic and social rights (including labor rights), the rights of women, and racial discrimination (including against indigenous peoples and minorities).

For the suggested reprisals risk assessment for IAMs, the following Treaty Bodies are particularly important:

- The **Human Rights Committee** supervises the implementation of the International Covenant on Civil and Political Rights (covering, among others, the rights to freedom of opinion and expression, assembly, and association).

  > http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx

- The **Committee on Economic, Social and Cultural Rights** supervises the implementation of the Covenant on Economic, Social and Cultural Rights (covering, among other things, labor rights, including the right to establish trade unions and adequate standards of living).

  > http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx

- The **Committee on the Elimination of All Forms of Racial Discrimination (CERD)** supervises the Treaty on the Elimination of All Forms of Racial Discrimination (covering racial discrimination, including against indigenous peoples and ethnic minorities). All States parties are required to submit regular reports in the form of "concluding observations" which are a valuable source of information.

> https://www.ohchr.org/EN/HRBodies/CERD/Pages/CERDIndex.aspx

- The **Committee against Torture** supervises the implementation of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. Since 2009, the Committee has sent letters to State Parties on alleged reprisals against persons or groups that have sought to interact with the Committee

> https://www.ohchr.org/EN/HRBodies/CAT/Pages/CATIntro.aspx
https://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/TBSearch.aspx?Lang=en&TreatyID=1&DocTypeID=130

Each Treaty Body review is based on the State parties' reports, information received from national human rights institutions and CSOs, and an interactive dialogue with civil society and the State party in Geneva. The information submitted by the national human rights institution and CSOs for the review contains particularly useful information. This information, together with the results of all country reviews, is available at each of the Treaty Bodies website and can easily be found through accessing the search function for sessions of the Treaty Body through the websites of respective body.

The reporting of the UN Treaty Bodies will contain only part of the information necessary for the IAMs to assess the risks of reprisal in the country. For example, the reviews by the Human Rights Committee may address broader key human rights issues of relevance, such as freedom of expression and opinion, but may not specifically cover the situation of human rights defenders. The information may also be outdated, as many States tend to be significantly behind schedule in their reporting to the Treaty Bodies.

Human Rights Watch
Human Rights Watch is a non-profit, nongovernmental human rights organization made up of roughly 400 staff members around the globe, including country experts, lawyers, journalists, and academics of diverse backgrounds and nationalities. The organization's annual reports contain useful and up-to-date information about human rights defenders and the climate for CSOs.

> https://www.hrw.org/world-report/2016#

Inter-American Commission on Human Rights (IACHR)
Information produced by the Inter American Human Rights system – the Inter-American Commission (and the associated Inter-American Court on Human Rights) – can be useful for understanding broader human rights issues, and the specific situation of human rights defenders in member countries of the Organization of American States (OAS). The Commission's country reports concerning the human rights situation in OAS member states is important in this regard.

> http://www.oas.org/en/iachr/reports/country.asp

The precautionary measures system through which the Commission can request member states to take measures to protect specific individuals or groups at risk will also be important for the IAMs to consult. In cases involving grave and urgent situations, the Commission can ask States to adopt urgent measures to prevent irreparable harm. It may also request information and issue recommendations. In addition, in the case of extremely grave and urgent situations, the IACHR may ask the Inter-American Court to order States to adopt provisional measures to prevent irreparable harm. Currently, around one-third of the precautionary measures granted by the Inter-American Commission every year are intended to protect the life and integrity of human rights defenders and justice operators in the region.

A list of current precautionary measures adopted by the Inter-American Commission is available at http://www.oas.org/en/iachr/decisions/precautionary.asp. The list of precautionary measures could be consulted by the IAMs to ascertain whether requesters or others associated with them have had precautionary measures issued on their behalf, or if there are others in the project area of influence under such protection.[120]

The Office of the Rapporteur on the situation of human rights defenders also provides support in the specialized analysis of petitions presented to the Inter-American Commission regarding the situation of human rights defenders.

> http://www.oas.org/en/iachr/defenders/default.asp

International Service for Human Rights (ISHR)
The International Service for Human Rights is a Geneva-based CSO working to support human rights defenders, with particular expertise in advocacy relating to reprisals against persons seeking to cooperate with the UN and the African Commission on Human and Peoples Rights. The organization regularly brings instances of reprisals to the attention of these bodies.

> http://www.ishr.ch/news/protecting-human-rights-defenders-reprisals

Peace Brigades International (PBI)
PBI has been working to support human rights defenders for more than 30 years. Its observers provide protective accompaniment to local human rights defenders whose lives and work are under threat. Through its field presences, PBI also publishes well-regarded analysis of national level protection programs.

> https://www.peacebrigades.org

120 - Note, however, that the Commission rarely shares information about granted precautionary measures to ensure that the safety of the persons concerned is not furthered jeopardized.

Protectdefenders.eu
Protectdefenders.eu is the European Union's Human Rights Defenders mechanism, established to protect defenders at high risk and facing the most difficult situations worldwide. It is a consortium of 12 international and regional human rights organizations that collectively implement the European Human Rights Mechanism. Through its global mapping of instances of reprisals, IAMs have access to a database with specific information on country-specific instances of reprisals, including their frequency and the forms that they have taken.

> https://www.protectdefenders.eu/en/stats.html?-yearFilter=2017&regionFilter=af&countryFilter=-BI#mf

Protection International (PI)
Based in Brussels, the CSO Protection International has been monitoring the situation of human rights defenders since 1998. In addition to capacity building for defenders through "protection desks," PI regularly publishes analysis of national level protection programs for human rights defenders and their effectiveness.

> https://www.protectioninternational.org/en/node/1537

Office of the UN High Commissioner for Human Rights (OHCHR)
The High Commissioner for Human Rights is principal human rights official of the UN. The High Commissioner is supported by a secretariat, based in Geneva, and has extensive presence in the field. As part of annual reporting to UN bodies or at the direct request of those bodies, OHCHR in the field routinely produces reports on country situations. These reports contain up-to-date information about the human rights situation in the country and cover several components of the suggested risk assessment template. A list of field presences of the OHCHR, their reporting mandates, and their reports is available at http://www.ohchr.org/EN/Countries/Pages/WorkInField.aspx. As noted, the UN OHCHR has a Senior Official on UN Systemwide Efforts to address reprisals, which can be reached here: reprisals@ohchr.org

UN Secretary General Annual Reporting on Reprisals
Since 2010, the UN Secretary General has issued reports annually on reprisals against individuals and groups seeking to cooperate with the UN in the field of human rights. These reports include specific references to the countries in which reprisals have happened, and the UN's response to address them. The reports are compiled by the UN Human Rights Office (OHCHR).

> https://www.ohchr.org/EN/Issues/Reprisals/Pages/Reporting.aspx

While the cases of intimidation and reprisals are increasing, CSOs working to support human rights defenders have noted that the number of cases reported to and by the UN remain low. The low number reflects the fact that not all cases are reported to OHCHR, either due to lack of awareness of the report's existence, or fear of further reprisals. It also reflects the fact that OHCHR will not include cases where the affected person's situation could be made worse if his/her case is publicly reported.

UN Special Rapporteurs or Working Groups – Special Procedures of the Human Rights Council
Special procedures are independent individuals and/or working groups that have been appointed by member states in the UN Human Rights Council. They have a mandate to analyze and report on human rights situations in specific countries and/or thematic issues.[121]

Special procedures of most relevance for the IAM risk assessment include:

- The Special Rapporteur on the situation of human rights defenders (http://www.ohchr.org/en/Issues/SRHRDefenders/Pages/SRHRDefendersIndex.aspx)

120 - A list of the current country mandates and their terms can be found at http://spinternet.ohchr.org/_Layouts/SpecialProceduresInternet/ViewAllCountryMandates.aspx

- The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN Doc. A/HRC/29/32) (http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx)

- The Special Rapporteur on the rights to freedom of peaceful assembly and of association (http://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/SRFreedomAssemblyAssociationIndex.aspx)

- Special Rapporteurs with a country-specific mandate (http://spinternet.ohchr.org/_Layouts/SpecialProceduresInternet/ViewAllCountryMandates.aspx).

Special procedures fulfil their mandates by, among others:

- Undertaking country visits to assess the situation of the thematic human right(s) or country human rights situation, depending on their mandate. These reports are made publicly available on their websites.[122]

- Acting on individual cases and concerns of a broader, structural nature by sending communications to States and non-State actors (for example business enterprises) in which they bring alleged violations or abuses to their attention and seek clarification on allegations that they have received.

Since 2011, the special procedures have submitted a joint report on their communications to each regular session of the Human Rights Council. These periodic reports include short summaries of allegations communicated to States or other entities, with hyperlinks to the text of the communications sent and responses received.

> http://www.ohchr.org/EN/HRBodies/SP/Pages/CommunicationsreportsSP.aspx

Universal Periodic Review (UPR) of the UN Human Rights Council

The UPR is a peer review process voluntarily undertaken on a 4- to 5-year cycle in the UN Human Rights Council reviewing the human rights records of all UN member states. Official information from the State, UN data and reports, and information from CSOs and other stakeholders are submitted as part of the database for the review.

Of particular relevance for the IAM risk assessment is the UN compilation report, which is submitted for each country's review. This report is divided into thematic sections and contains a summary of recommendations issued by all UN human rights bodies for the country concerned. Similarly, the CSO compilation report contains a useful summary of all the submission of CSOs for the country review, with references to the individual or joint CSO submissions that are accessible on the same site.

All documentation regarding the UPR is publicly available and searchable by country at http://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx. The website operated by the CSO UPR-info (https://www.upr-info.org/en) also has easily accessible resources related to each of the country reviews, including dates for the upcoming reviews.

2. Further guidance for the risk assessment template

The risk assessment template suggested in this toolkit is a simplified adaptation of the risk assessment models developed by Protection International, Front Line Defenders, Tactical Technology Collective, and the UN Human Rights Office. IAMs are encouraged to familiarize themselves with these assessments and associated guidance, as they provide important additional detail and advice for how to systematically assess security situations and develop strategies and tactics to reduce risks.

122 - Country reports are available at the Special Rapporteurs' dedicated websites (maintained by the UN Human Rights Office), which can be accessed through http://www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx.

Front Line Defenders
Workbook on Security: Practical Steps for Human Rights Defenders at Risk, 2016.

> https://www.frontlinedefenders.org/en/resources-publications-opportunity

Protection Handbook for Human Rights Defenders, 2016.

> https://www.frontlinedefenders.org/en/resource-publication/protection-handbook-human-rights-defenders

Office of the UN High Commissioner for Human Rights.
Manual on Human Rights Monitoring, in particular Chapter 14: Protection of Victims, Witnesses and Other Cooperating Persons.

> http://www.ohchr.org/Documents/Publications/Chapter14-56pp.pdf

Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law, 2015.

> https://www.ohchr.org/Documents/Publications/CoI_Guidance_and_Practice.pdf

Protection International
New Protection Manual for Human Rights Defenders, 2009, by Eguren and Marie Caraj.

> https://www.protectioninternational.org/en/node/1106

Tactical Technology Collective
Holistic Security – A Trainer's Manual, 2016.

> https://holistic-security.tacticaltech.org/trainers-manual

Holistic Security – An Interactive Website with Guides to Assessing Risks and Responding to Threats.

> https://holistic-security.tacticaltech.org/

APPENDIX 2. EXTERNAL RESOURCE ORGANIZATIONS

Organization	What it is and what it can do	Website
Arab Human Rights Fund	A nonprofit organization that provides support for the promotion and realization of all human rights in the Arab region. It provides financial and technical support to individual human rights defenders and organizations in the Arab region.	http://www.ahrfund.org/new/en/mission-and-objectives
Arab Programme for Human Rights Activists	Supports continuous, collective dialogue on the problems, needs and aspirations of human rights activists in the Arab world. In urgent situations, the organization organizes meetings with concerned ambassadors to solicit support for the individuals at risk.	http://aphra.org.eg/wordpress/en/home/
Article 19	Works on freedom of expression and freedom of information. Undertakes litigation in international and domestic courts on behalf of individuals or groups whose rights have been behalf of individuals or groups whose rights have been violated. Provides legal and professional training.	https://www.article19.org/
Asian Centre for Human Rights	Works to protect human rights in Asia, including increasing the capacity of human rights defenders and civil society groups through trainings on national and international human rights procedures, and providing legal, political, and practical advice for defenders.	http://www.achrweb.org/

CAIRO Institute for Human Rights Studies	Assists with professional development for human rights defenders in the Arab region.	https://cihrs.org/?lang=en
Civil Rights Defenders	Supports and empowers human rights defenders at risk on four continents and has pioneered the first security alarm system for human rights defenders through the Natalia Project. Since 2011, Civil Rights Defenders has operated an Emergency Fund to help human rights defenders who face significant pressure or threats.	https://crd.org/
East and Horn of Africa Human Rights Defenders Project (EHAHRDN)	Represents more than 70 organizational and individual members. The EHAHRDN runs a protection program that can provide emergency assistance and protection for individuals at risk on a case-by-case basis.	https://www.defenddefenders.org/
FIDH (International Federation for Human Rights)	In partnership with the World Organization Against Torture (OMCT), FIDH runs the Observatory for the Protection of Human Rights Defenders, through which it takes action in support of individuals who are exposed to reprisals as a result of their human rights activities. These actions include issuing and distributing urgent alerts in six languages, provision of emergency grants (medical, psychological, and legal support; help with relocation) and capacity grants, prison visits, judicial observation and defence, national and international advocacy, investigative missions, public campaigns on social media and the internet, urgent advocacy directed at actors of social change, and initiating legal and paralegal recourse.	https://www.fidh.org/en/issues/human-rights-defenders/#

Front Line Defenders	Offers a number services for individuals at risk, including advocacy, which can entail sending information to the UN or to other regional mechanisms and liaising with EU embassies under the EUs guidelines on human rights defenders; protection grants provided under a very flexible program that reflect the defenders' needs (legal fees, medical support, relocation, hard security measures, etc.); training and capacity building for defenders and their organizations on security measures, including digital security; rest and respite services, whereby defenders are invited to come and rest (or work) for a defined period in Dublin or elsewhere (ranging from days to months); and an emergency contact (24/7) service.	https://www.frontlinedefenders.org/
FORUM ASIA's Human Rights Defenders program	A protection measure for human rights defenders and women human rights defenders in Asia. It provides practical safeguards for defenders at risk by reducing both actual and perceived threats stemming from their work and activities.	https://www.forum-asia.org/
Fund for Global Human Rights	Supports frontline organizations and dispenses grants to support campaigns that otherwise might falter for lack of resources.	http://globalhumanrights.org/
Human Rights House Network	Protects and supports human right defenders and their organizations in 15 countries in Western Balkans, Eastern Europe and South Caucasus, East Africa and the Horn of Africa, and Western Europe.	http://humanrightshouse.org/

Lifeline Embattled CSO Assistance Fund	Provides emergency financial assistance to civil society organizations under threat or attack, and rapid response advocacy grants targeting broader threats to civil society.	https://www.csolifeline.org/
Peace Brigades International (PBI)	Provides protection, support, and recognition to local human rights defenders who work in areas of repression and conflict and have requested such support. It offers protection to defenders primarily through its protective accompaniment, which is done upon the request of human rights defenders themselves. PBI also organizes security trainings workshops, which are delivered by local partner organizations with extensive experience.	https://www.peacebrigades.org/en/about-pbi/what-we-do/protective-accompaniment
Protection International	Based in Brussels, Protection International provides capacity-building for defenders through so-called protection desks.	https://www.protectioninternational.org/
Protectdefenders.eu	The European Union's Human Rights Defenders mechanism, established to protect defenders at high risk and facing the most difficult situations worldwide. It is implemented by a consortium of 12 international and regional human rights organizations and includes a variety of rapidly disbursed grants, including temporary relocation and other emergency grants.	https://protectdefenders.eu
Office of the United Nations High Commissioner for Human Rights (OHCHR)	The principal human rights official of the United Nations. With a global mandate, the High Commissioner is serviced by an Office (OHCHR), based in Geneva and its extensive presence at the regional and country level. OHCHR's field presences can provide important protection channels for individuals at risk.	http://www.ohchr.org/EN/Countries/Pages/WorkInField.aspx

Urgent Action Fund for Women's Human Rights	A global women's fund that can intervene quickly when activists are poised to make great gains or face serious threats to their lives and work. It offers online, text, and mobile funding applications to respond to requests from women's human rights defenders within 72 hours and have funds on the ground within 1–7 days.	https://urgentactionfund.org/apply-for-a-grant/

Note: The inclusion of any organization in this list is not meant to be considered an endorsement by the institutions that have commissioned this publication.

PHOTO: TOM BRICKS

APPENDIX 3. ADDITIONAL RESOURCES

The Adidas Group
The Adidas Group and Human Rights Defenders, 2016.

> https://www.adidas-group.com/media/filer_public/f0/c5/f0c582a9-506d-4b12-85cf-bd4584f68574/adidas_group_and_human_rights_defenders_2016.pdf

African Development Bank
Whistle-blowing and Complaints Handling Policy, 2007.

> https://www.afdb.org/fileadmin/uploads/afdb/Documents/Policy-Documents/18136242-EN-WHISTLE-BLOWING-POLICY-FINAL-FINAL-WKF.PDF

Association for the Prevention of Torture
Monitoring Places of Detention – A Practical Guide, 2004.

> https://www.apt.ch/content/files_res/monitoring-guide-en.pdf

Briefing No. 4: Mitigating the Risks of Sanctions related to Detention Monitoring, 2012.

> https://apt.ch/content/files_res/Briefing4_en.pdf

Centre for Humanitarian Dialogue
Proactive Presence: Field Strategies for Civilian Protection, 2006, by L. Mahoney.

> http://www.globalprotectioncluster.org/_assets/files/tools_and_guidance/protection-cluster-coordination-toolbox/proactivepresence_chd.en.pdf

Coca-Cola Company
Coca Cola: Suppliers and Customer Partnerships.

> https://www.coca-colacompany.com/our-company/suppliers/supplier-and-customer-partnerships

Compliance Advisor Ombudsman (CAO)
Approach to Responding to Concerns of Threats and Incidents of Reprisals, 2017.

> http://www.cao-ombudsman.org/documents/CAO-Reprisals-web.pdf

Corporate Social Responsibility Initiative
Due Diligence for Human Rights: A Risk-Based Approach, 2009, by Mark B. Taylor, Luc Zandvliet, and Mitra Forouhar (Working Paper No. 53).

> https://sites.hks.harvard.edu/m-rcbg/CSRI/publications/workingpaper_53_taylor_etal.pdf

Electronic Frontier Foundation, Surveillance Self-Defense
Tips, Tools and How-to's for Safer Online Communication.

> https://ssd.eff.org/en/

Front Line Defenders
Workbook on Security: Practical Steps for Human Rights Defenders at Risk, 2016.

> https://www.frontlinedefenders.org/en/resources-publications-opportunity

Protection Handbook for Human Rights
Defenders, 2016.

> https://www.frontlinedefenders.org/en/resource-publication/protection-handbook-human-rights-defenders

Government of Norway
Guidelines for Observation and Exclusion from the Government Pension Fund Global. 2017.

> https://www.regjeringen.no/globalassets/upload/fin/statens-pensjonsfond/formelt-grunnlag/guidelines-for-observation-and-exclusion-from-the-gpfg---17.2.2017.pdf

European Bank for Reconstruction and Development
Agreement Establishing the European Bank for Reconstruction and Development, 1990.

> https://www.ebrd.com/news/publications/institutional-documents/basic-documents-of-the-ebrd.html

Inter-American Development Bank
Inter-American Development Bank Series on Environmental and Social Risk and Opportunity: Meaningful Stakeholder Consultation, 2017.

> https://publications.iadb.org/bitstream/handle/11319/8454/Meaningful-Stakeholder-Consultation.pdf?sequence=3

International Service for Human Rights
Reprisals Handbook, 2018.

> https://www.ishr.ch/news/reprisals-new-ishr-handbook-reprisals-human-rights-defenders

New South Wales Ombudsman
Guidelines on Confidentiality, 2011.

> https://www.ombo.nsw.gov.au/__data/assets/pdf_file/0011/3602/Guideline-C7-Confidentiality.pdf

Office of the UN High Commissioner for Human Rights
Manual on Human Rights Monitoring, in particular Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons.

> http://www.ohchr.org/Documents/Publications/Chapter14-56pp.pdf

Manual on Human Rights Monitoring, Chapter 30: Using Presence and Visibility.

> http://www.ohchr.org/Documents/Publications/Chapter30-20pp.pdf

Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law.

> https://www.ohchr.org/Documents/Publications/CoI_Guidance_and_Practice.pdf

Special Procedures of the UN Human Rights Council. Revised terms of reference for country visits by Special Procedures Mandate holders of the United Nations Human Rights Council (based on Appendix V, E/CN.4/1998/45) (June 2016).

> http://www.ohchr.org/Documents/HRBodies/SP/ToRs2016.pdf

Special Procedures Mandate holders of the United Nations Human Rights Council, 2016. Revised terms of reference for country visits.

> http://www.ohchr.org/Documents/HRBodies/SP/ToRs2016.pdf

UN Sub-Committee on prevention of torture and other cruel, inhuman or degrading treatment or punishment: Policy on reprisals in relation to its visiting mandate (31 May 2016). UN Doc. CAT/OP/6/Rev.1.

> http://tbinternet.ohchr.org/Treaties/CAT-OP/Shared%20Documents/1_Global/CAT_OP_6_Rev-1_7759_E.pdf

UN Committee against Torture. *Guidelines on the Receipt and Handling of reprisals against individuals and organizations cooperating with the Committee against Torture under articles 13, 19, 20 and 22 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, UN Doc. CAT/C/55/22 (September 2015).

UN Human Rights Treaty Bodies, 2015. *Guidelines against intimidation or reprisals adopted at the twenty-seventh meeting of chairpersons of the human rights treaty bodies* (San Jose Guidelines). UN Doc. HRI/MC/2015/6.

> http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=HRI/MC/2015/6&Lang=en

Pan American Health Organization/World Health Organization
Methodologies for Information Sharing and Knowledge Management in Health How to Organize and Preserve the Institutional Memory, 2015.

> https://www.paho.org/hq/index.php?option=com_docman&task=doc_view&Itemid=270&gid=35630&lang=fr

Protection International
New Protection Manual for Human Rights Defenders, 2009, by Enrique Eguren and Marie Caraj.

> https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

CUIDÁNDONOS: Guía de protección para defensoras y defensores de derechos humanos en áreas rurales, 2015.

> https://www.protectioninternational.org/es/node/1103

SANS Institute
History of Encryption. 2001.
Tactical Technology Collective
Holistic Security, 2016. Available at

> https://holistic-security.tacticaltech.org/

Holistic Security: A Trainer's Manual, 2017.

> https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/60/holisticsecurity_trainersmanual.pdf

Tactical Technology Collective and Front Line Defenders
Security-in-a-box, by Wojtek Bogusz, Dimitri Vitaliev, and Chris Walker, 2009–present,

> https://securityinabox.org/en/guide/secure-communication

United Nations
Effective Mediation – issues an Annex to the report of the Secretary General on Strengthening the role of mediation in the peaceful settlement of disputes, conflict prevention and resolution (A/66/811, 25 June 2012).

United Nations Institute for Training and Research, Department of Political Affairs
A Manual for UN Mediators – Advice from UN Representatives and Envoys, 2010.

University of Colorado
Shuttle Diplomacy/Mediated Communication, by Heidi Burgess and Guy Burgess, 2003.

> http://www.intractableconflict.org/www_colorado_edu_conflict/peace/treatment/shuttle.htm accessed July 17, 2003.

The World Bank
Inspection Panel: Guidelines to Reduce Retaliation Risks and Respond to Retaliation during the Panel Process, 2016.

> http://inspectionpanel.org/sites/ip-ms8.extcc.com/files/documents/IPN%20Retaliation%20Guidelines_2018.pdf

PHOTO: PEXELS

www.iadb.org/mici

IAMnet Independent Accountability Mechanisms Network

independentaccountabilitymechanism.net