

# Reprisal Risk Management

Tove Holmström

Environmental and Social  
Solutions Unit

TECHNICAL  
NOTE N°  
IDB-TN-2434

# Reprisal Risk Management

Tove Holmström

April 2022



Cataloging-in-Publication data provided by the  
Inter-American Development Bank  
Felipe Herrera Library

Holmström, Tove

Reprisal Risk Management / Tove Holmström.

p. cm. — (IDB Technical Note ; 2434)

Includes bibliographic references.

1. Project management-Evaluation. 2. Project management-Methodology. 3.

Participatory monitoring and evaluation (Project management)-Analysis. I.

Inter-American Development Bank. Environmental and Social Solutions Unit. II. Title.

III.

Series.

IDB-TN-2434

JEL Codes: O54: O44

Keywords: Reprisals; Retaliation; Risk Management

<http://www.iadb.org>

Copyright © 2022 Inter-American Development Bank. This work is licensed under a Creative Commons IGO 3.0 Attribution-NonCommercial-NoDerivatives (CC-IGO BY-NC-ND 3.0 IGO) license (<http://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) and may be reproduced with attribution to the IDB and for any non-commercial purpose. No derivative work is allowed.

Any dispute related to the use of the works of the IDB that cannot be settled amicably shall be submitted to arbitration pursuant to the UNCITRAL rules. The use of the IDB's name for any purpose other than for attribution, and the use of IDB's logo shall be subject to a separate written license agreement between the IDB and the user and is not authorized as part of this CC-IGO license.

Note that link provided above includes additional terms and conditions of the license.

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.



This publication on Reprisal Risk Management was prepared under the leadership of Oscar Came, Acting Unit Chief of the Environmental and Social Solutions Unit (ESG) at the Inter-American Development Bank. The publication was written by Tove Holmström. A former staff member of the UN Human Rights Office, Tove Holmström is an independent human rights consultant based in Paris, France. Her work addresses responsible business conduct with a particular focus on retaliation against stakeholders.

The core team consisted of Soraya Senosier, Julio Rojas and Juan Martinez. Reviews and valuable comments on drafts were made by ESS environmental and social specialists. Valuable comments and suggestions were received from the IDB's Vice Presidency for Sectors, Sector Managers, Independent Consultation and Independent Mechanism (MICI), and IDB Invest.

## Executive summary

In September 2020 the Board of Executive Directors of the Inter-American Development Bank (IDB) approved a new Environmental and Social Policy Framework (ESPF). The ESPF reflects the IDB's zero tolerance to "retaliation, such as threats, intimidation, harassment, or violence, against those who voice their opinion or opposition to an IDB-financed project or to the Borrowers".<sup>1</sup> Stand-alone ESPF standards on labour, gender equality, community health and safety, and stakeholder engagement also place obligations on borrowers to proactively identify and prevent or mitigate risks of reprisals against project stakeholders, including project-affected people (PAP)<sup>2</sup> and project workers.<sup>3</sup>

In the context of IDB-funded projects, PAP or third parties associated with them may have diverging views from borrowers on the need for a given project, its chosen location and/or specific aspects of its design and/or implementation. In these types of situations, risks of behaviour that may amount to retaliation – such as verbal threats, physical violence or discrimination in relation to employment – may materialise.

It should be noted that in the context of IDB-funded projects, IDB's role is to support Borrowers in the development and implementation of IDB-financed projects that are environmentally and socially sustainable, and to enhancing the capacity of Borrowers' environmental and social (E&S) frameworks to assess and manage the environmental and social risks and impacts of projects including in relation to risks of retaliation against project stakeholders. As such, the technical note seeks to increase awareness of risks of retaliation among both IDB staff as well as Borrowers and Executing Agencies. It also supports IDB staff, in their supervisory and advisory role vis-à-vis IDB projects and the E&S capacity of Borrowers and Executing agencies,<sup>4</sup> as well as Borrowers and Executing Agencies to identify, evaluate and

---

<sup>1</sup> Inter-American Development Bank, 2020. Environmental and Social Policy Framework, Part 1, Section 7.2.

<sup>2</sup> Stakeholder refers to individuals, or groups, including local, downstream, and transboundary communities, who (i) are affected or likely to be affected by the project ("project-affected people") and (ii) may have an interest in the project ("other stakeholders").

<sup>3</sup> The ESPF defines project workers as: (i) people employed or engaged directly by the Borrower (including the project proponent and the project implementing agencies) to work specifically in relation to the project (direct workers); (ii) people employed or engaged through third parties to perform work related to core functions of the project for a substantial duration (contracted workers); and (iii) workers engaged by the Borrower's primary suppliers (primary supply workers). This includes full-time, part-time, temporary, seasonal, and migrant workers. Migrant workers are workers who have migrated from one country to another or from one part of the country to another for purposes of employment.

<sup>4</sup> As noted in the ESPF (3.13), the role of the IDB is (i) screen and classify operations according to environmental and social impact and assign an environmental and social risk classification; (ii) review the information provided by the Borrower relating to the environmental and social risks and impacts of the project and request additional and relevant information where there are gaps that prevent the Bank from completing its due diligence; (iii) undertake its own due diligence of proposed projects and of project changes throughout the project lifecycle, proportionate to the nature and potential significance of the environmental and social risks and impacts related to the project; (iv) as and where required, support the Borrower in carrying out early and continuing engagement and meaningful consultation with stakeholders, specifically affected communities, and in developing project-based grievance mechanisms; (v) assist the Borrower in identifying appropriate methods and tools to assess and manage potential environmental and social risks and impacts at the project level; (vi) agree with the Borrower on the conditions under which the Bank is prepared to provide support to a project, as set out in the Environmental and Social Action Plan (ESAP); (vii)

address risks of retaliation over the course of project design, implementation, monitoring and closure. By building on the requirements of the Bank's Stakeholder Engagement Environmental and Social Performance Standard (ESPS 10) in particular, the note provides a framework for identifying, assessing, preventing, mitigating risks of reprisals, and responding to allegations that reprisals have occurred in the context of public sector projects.

In light of ESPF requirements, this technical note focuses in particular on managing risks of reprisals in the context of developing and implementing stakeholder engagement plans and seeking to resolve grievances that may arise over in relation to project design and implementation. However, it should be noted at the outset that an inclusive and robust stakeholder engagement plan is not the golden ticket to prevent risks of retaliation against project stakeholders: risks are unique to each project, context and moment, and additional measures will often be needed. Measures to prevent or reduce risks of reprisals against project stakeholders should be developed and implemented in close consultation and with the informed consent, of those at risk, as should any responses to responding to any allegations that reprisals have occurred. In short, the ESPF and this accompanying technical note should be read as a starting point for addressing risks of reprisals against project stakeholders, rather than as a blueprint for managing risks.

The technical note proceeds in four parts:

1. Part I elaborates what is understood by the term reprisals and who common victims and perpetrators are in the context of development finance projects. This part also outlines key IDB ESPF requirements relating specifically to identifying, preventing and addressing risks of reprisals against PAP individuals and communities and national legal and policy frameworks that similarly focus on the prevention of, and appropriate responses to, retaliation.
2. To inform an evaluation of the level of risk of retaliation, part II provides an overview of some of the key contextual risk factors that make retaliation in a given project more likely and that merit heightened due diligence to prevent or reduce the likelihood that such risks materialise, including:
  - Country level factors (the extent to which civic space can operate freely)
  - Risks associated with past track-records of executing agencies or other key business relationships with a key role in project design and implementation (contractors, sub-contractors, consultants, suppliers) of past instances of retaliation against PAPs.
  - Potential tensions and distrusts between local authorities and PAPs in the project area / project area of influence.
  - Tensions within or between PAP communities, including in relation to perceived project risks and impacts as well as benefits.

---

monitor the environmental and social performance of a project in accordance with the requirements established in the Loan Agreement, the ESAP and the ESPS; and (viii) disclose environmental and social documentation produced by the Borrower and the Bank.

3. Part III provides a number of baseline measures that can be taken in relation to preparing and implementing stakeholder engagement plans (executing agencies) and evaluating the quality of such plans (IDB) in a way that seeks to understand the views and perspectives of those critical of the project and that solicits stakeholder feedback on an ongoing basis in a way that does not expose PAPs to risks for expressing their views freely.
4. Part IV provides guidance on how to respond to allegations that reprisals have taken place, suggesting a three-step approach that includes: receiving and reviewing information, ensuring confidentiality of the victim(s) and acting immediately where allegations are serious; discussing and agreeing with victim(s) on measures to respond to reprisal (alone or in collaboration with other actors) and how, when and by whom the measures will be implemented; and communicating with victim(s) on the implementation of agreed measures to respond to the allegations and considering the situation active until the victim reports that he/she is safe.

This technical note and the measures it proposes have been informed by four key premises:

- **There is no zero-risk project.** The absence of indications of retaliation is no guarantee of what might be happening or what may happen in the future. Retaliation against project stakeholders can be an issue in any project, although some contextual and project-level risk factors create conditions that increase the likelihood of reprisals (see chapter II of the present note). Similarly, while risks of reprisal can never be reduced to zero, they can be significantly lessened through appropriate prevention and mitigation measures that should be part and parcel of a robust stakeholder engagement plan.
- **Prevention is essential.** This note focuses on preventative measures as the most appropriate means to counter risks. A good prevention strategy should be prioritized in high-risk projects, and additional due diligence efforts and funding should be ensured to ensure that it can be implemented accordingly.
- **Those that have been identified as being at risk of retaliation should be an integral part of any prevention efforts and of any responses to address reprisals that have occurred.** Existing local knowledge should feed into any risk assessments, and into the design of mitigation measures and responses to allegations of retaliation. To the extent possible, any responses or measures to potential reprisals should be agreed with those at risk at the outset before reprisals have happened. Community-based partners – in particular local community leaders and organisations with local presence or expertise – are also an important resource for identifying and managing risks and responding to incidents as these arise.
- **Measures to respond to allegations of retaliation may need to involve a number of stakeholders – not only the IDB but organisations with particular expertise in the protection of individuals and groups at risk.** Therefore, in projects where risks of reprisal are deemed significant, efforts should be made early on, ideally already during the project design and negotiation phase, to contact and coordinate with such agencies.

# Table of contents

- Executive summary..... 2
- 1. Introduction ..... 6
- 2. Identify and assess risks of reprisal ..... 17
- 3. Prevent or mitigate risks of reprisal ..... 24
- 4. Address and respond to allegations of retaliation ..... 42
- Annex I. Overview of potential support organisations for risk mitigation measures and responses to reprisals ..... 49
- Annex II: Illustrative overview of national laws of relevance for retaliation risk management..... 55
- Additional reading..... 59



## 1. Introduction

The following section introduces the topic of reprisals against project stakeholders. It elaborates what reprisals are (see Box 1), who is typically impacted and who the common authors of reprisals, in a development finance context, are. It also outlines IDB's zero-tolerance expectations with regards reprisals, as expressed in the ESPF, and provides a snapshot of some of the legal standards or policy frameworks in many of IDB's countries of operation that require the identification, prevention and/or mitigation of reprisals risks.

### Box 1. What is a reprisal?

Reprisal refers to any acts that impairs or harms (or threatening to impair or harm) project stakeholders, directly or indirectly, with the intent to influence improperly the actions of those stakeholders in connection with an IDB project. Typically, acts of reprisal are taken against project stakeholders who have expressed critical views concerning, or opposition to, Bank-funded projects or Borrowers/Executing Agencies.

Common acts of reprisals include intimidation, threats, harassment, punishment, judicial proceedings, or any other retaliatory acts against those who voice their opinion or opposition to an IDB-financed project, to a third party related to the project, or to the Borrower.

Other terms commonly used to refer to reprisal are sanction, reprimand, and retaliation.

In recent years, reports of reprisal against individuals, communities and organisations that express concerns and make complaints relating to the activities of international finance institutions have increasingly made international headlines. These reports take place against a global backdrop of growing restraints on civic space that restrict the possibility of individuals and groups to organise, participate and communicate with each other freely and without hindrance and to express their concerns and grievances without being subject to threats or other forms of retaliation by State- or non-State actors. Increasing levels of impunity across the globe also contributes to a context in which reprisals are at rise as perpetrators of various forms of retaliation – including killings – are less likely to be brought to justice.

Reprisals against individuals and communities that voice concerns about business-related human rights impacts is a serious concern in Latin America: in 2020, for example, available data suggests that of the 604 reported killings of human rights defenders at the global level, most were concentrated to Latin America (194 attacks).<sup>5</sup> Land and environmental rights defenders, in particular, were killed in high numbers in the region, with almost 3 in 4 of the 227 fatal attacks recorded having

---

<sup>5</sup> See <https://www.business-humanrights.org/en/from-us/briefings/line-fire-increased-legal-protection-needed-attacks-against-business-human-rights-defenders-mount-2020/>

taken place in the Americas.<sup>6</sup> It should be noted, however, that while more reports of retaliation are surfacing – in part due to the establishment of dedicated channels for providing such information – the real extent is likely to be much higher. Numbers are underreported due to a lack of awareness of those impacted of channels available for reporting incidents or out of fear of being subject to further retaliation if reports become public. Where information is available, it typically focuses on the most serious forms of retaliation, such as legal harassment or physical violence, and less so on other more subtle forms, such as, for example, defamation and slander or loss employment-related opportunities.

In Latin-America and the Caribbean, indigenous peoples, Afro-descendant communities and other groups with customary land tenure patterns have been reported to be particularly at risk of reprisal.<sup>7</sup> This heightened risk corresponds to their generally marginalized position in society, and long-standing conflicts over land that may not be resolved or only partially resolved. Land-consuming projects that are planned or implemented on or in the vicinity of contested land areas and resources, such as hydro-dams or wind-energy projects, have the potential to exacerbate conflicts around land ownership and usage, and tend to be particularly challenging from a reprisal-risk point of view. In the region, women and LGBTQI individuals may also face additional risks of retaliation and the types of retaliation that they are subject to may be specific to their gender and/or sexual orientation. For example, women tend to be more susceptible to be subject to sexual harassment and gender-based violence and to slander that puts in question their respectability as a woman. Women's rights activists may encounter gender-specific obstacles when seeking to access effective remedies for reprisals that has been suffered, such as where community attitudes stigmatize sexual violence.<sup>8</sup>

### Retaliation in the context of development finance projects

In the context of development finance, acts of retaliation have, amongst other, encompassed verbal intimidation, slander and defamation, judicial harassment and criminalization (often referred to as strategic lawsuits against public participation, see box 1 below ), electronic or physical surveillance, property damage or loss, restrictions to freedom of movement, physical violence leading to bodily harm or fatality, as well as discrimination, disadvantage or adverse treatment in relation to employment or commercial contracts. Retaliation can often be covert, intangible and informal, making it difficult to identify and investigate. In corollary to this, the connection between an IDB project and reprisals that unfold against stakeholders may not be evident at first glance.

---

<sup>6</sup> Global Witness, Last Line of Defense (September 2021). 7 out of the 10 highest countries in terms of killings were located in Latin America. In Brazil and Peru, nearly three quarters of recorded attacks took place in the Amazon region of each country.

<sup>7</sup> An analysis of the work done by the Business and Human Rights Resource Centre in 2019 on individuals killed in 2019 is instructive: of the total reported number of 300 deaths, 40 % were engaged in advocacy related to land, environmental and indigenous peoples' rights. Most of the recorded attacks took place in Latin America (January 2020 Snapshot).

<sup>8</sup> United Nations Guidance Note on Protecting and Promoting Open Civic Space, September 2020, pg. 8.

Typically, where retaliation does occur, it is likely to involve a series of several incidents over time, often escalating from intimidation and threats that, if not addressed early on, end in more serious forms of reprisals. For example:

- An active trade unionist working for project-implementation agencies is demoted from her leadership position, then bullied and harassed by senior management for several months prior to being issued a notice for termination of her employment contract.
- A local community leader is portrayed in local media as a troublemaker and “anti-development” for opposing the development of a hydro-electric dam and receives multiple anonymous death threats prior to being shot.
- A leader of a non-governmental organisation working on environmental justice and who has openly criticized a development finance intermediary (DFI) project is denied the approval to re-register his organization and has unrelated assets frozen.
- The family member of an investigative journalist receives threatening calls and warnings for the journalist to not investigate claims of involuntary resettlement plans without due consultation with local communities in the context of public sector development finance projects. Following protracted digital surveillance and threats of revoking professional accreditation, the journalist is detained and subject to legal proceedings on grounds of libel and defamation (see Box 2, below, for additional information on strategic lawsuits against public participation).

## **BOX 2. STRATEGIC LAWSUITS AGAINST PUBLIC PARTICIPATION (SLAPPS)**

---

Strategic lawsuits against public participation (SLAPPs) generally refer to retaliatory lawsuits brought to silence individuals or organisations that have spoken out in the public sphere, often on issues relating to land use and land development issues. SLAPPs come with serious reputational costs for those affected, as they are stigmatised/ vilified by this type of legal action.

In the case of SLAPPs, the actual resolution of the plaintiffs' claims – for defamation, trespass, counterfeiting or related legal grounds – is a secondary motivation at best. SLAPPs are strategically used to deter critical speech by intimidating critics into silence. While these kinds of lawsuit may be dismissed as frivolous by courts of law, a SLAPP does not need to be successful in court to have its intended effect: they are typically effective because even a meritless lawsuit can take years and many thousands of dollars to defend, draining the resources and morale of those subjected.

A SLAPP can generally be detected by the following telltale signs:

- \* It targets fundamental rights and freedoms: The lawsuit targets activity that relates to freedom of speech, peaceful protest or petitioning of the government.
- \* It exploits a power-imbalance: The plaintiff is seeking to exploit its economic advantage to put pressure on the defendant(s).
- \* It threatens to bankrupt the defendant(s): the remedies sought are unusually aggressive or disproportionate to the conduct that is subject to the lawsuit.
- \* It attempts to remain in court for protracted periods of time: the plaintiff is engaged in procedural manoeuvres that appear intended to drag out the case or drive-up costs such as pursuing appeals with little prospect of success.
- \* It casts the net wide: the lawsuit targets individuals and the organisations for which the individuals work. The lawsuit is part of a wider public relations offensive designed to bully or intimidate critics.
- \* It follows a pattern of systematic harassment: the plaintiff has a history of threatening legal action or using SLAPPs to scare critics into silence.

Source: [\*Protect the protest – What is SLAPP?\*](#)

---

It should be noted that some project-stakeholders may already be 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 expressing critical views of DFI projects are easily blurred. Nevertheless, sharing concerns or criticism vis-à-vis projects may aggravate existing risks. In this regard, it has been noted that ensuring the protection of requesters and others associated with them is a shared responsibility of the State(s), borrowers and executing agencies, DFIs ,

their grievance mechanisms, the possible victims, and any other actors that can positively or negatively influence the safety of those at risk.<sup>9</sup>

Stakeholders' concerns for their safety, or the safety of their families or other associated persons, can also prevent them from speaking out about environmental and social risks and impacts associated with projects. In contexts where fear of reprisals is an issue, often because people have been punished for voicing concerns in the past, affected stakeholders and their representatives are more likely to engage in self-censorship, either by downplaying the concerns they may have about a project or deciding not to voice their concerns at all. Where this is the case, project-associated risks and impacts cannot be properly identified and/or responded to and, if they do materialise, can lead to increased costs and delays in implementation. As such ensuring stakeholder engagement free of retribution is an essential *sine qua non* for robust due diligence.

From an environmental and social standards' point of view, fear of retaliation also has a crippling effect on meeting key requirements on stakeholder engagement, including consultations with project affected people and implementing effective operational-level grievance mechanisms. Where risks of retaliation have not been addressed at the outset and incidents occur, project-affected parties are also likely to take their grievances elsewhere such as national or international media outlets, human rights organisations, independent accountability mechanisms or criminal justice institutions. As such, acts of reprisal can have serious reputational, financial and also potentially legal consequences both for IDB and for its clients. At a more foundational level, addressing risks of reprisals in a proactive manner is an important component of working towards ensuring a healthy civic space in which stakeholders feel at ease to share any concerns that they may have without routinely being subject to intimidation or other forms of retaliation. In this regard, the present note recognizes that risks of retaliation are intimately linked with the quality of civic space in any given country, and that promoting civic space, including but not limited to addressing risks of retaliation, is key to ensure that people feel comfortable to share their concerns about IDB projects (see Figure 1).

---

<sup>9</sup> 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.

**FIGURE 1** Open civic space will result in a variety of better outcomes

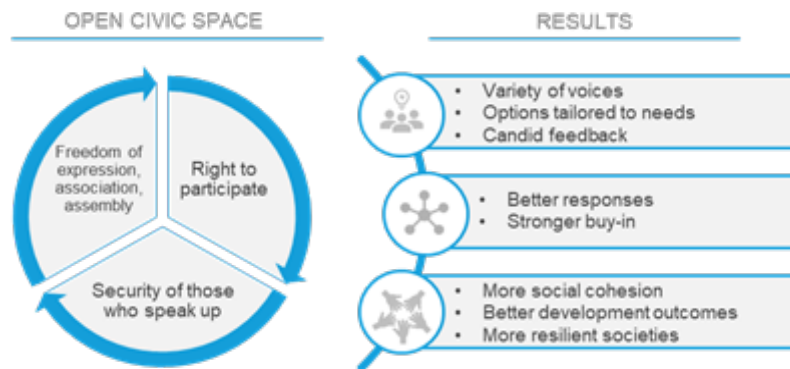


Figure 1. Open civic space. From the United Nations Guidance Note on Protection and Promotion of Civic Space (2020).

### At risk individuals and groups and potential perpetrators

While any project stakeholder may be at risk of retaliation for expressing concern over or outright opposition to a project, experience suggests that the following groups are particularly affected:

- Project affected people, in particular community leaders and their family members.
- Individuals or organisations that are working with project impacted communities to raise concerns, including civil society organizations, legal practitioners, and journalists.
- Requesters to IDB's independent accountability mechanism, the Independent Consultation and Investigation Mechanisms (the MICI), or others associated with them such as family members of individuals supporting their requests to the MICI (such as NGO representatives or lawyers) and local consultants that facilitate the work of the mechanism, including interpreters, translators, drivers, technical experts and "fixers" that work to ensure the smooth operations of the MICI.
- Labour organizers within the project workforce, including workers hired by contractors, sub-contractors, consultants, and suppliers, that express concern over work-practices associated with the project, in particular through workers' organisations (workers active in trade unions). Suppliers, contractors and consultants working on project design, implementation or monitoring and staff associated with the Borrower or implementing agency that raise concerns in relation to the project, can also suffer acts of retaliation, for example by the termination or non-renewal of contracts, demotion, loss of employment, or reputational damage with detrimental impacts on future employment offers. Where allegations concern corruption or maladministration, staff or contractors working in the functions of

procurement and financial management may be particularly susceptible to risks. In relation to this category of potential victims, national frameworks on the protection of whistle-blower protection may apply, in particular where the concerns raised relate to allegations of corruptions or maladministration.<sup>10</sup>

Potential perpetrators of retaliation can be any actor associated with a project, including current or former staff of government agencies at central or local levels, public security forces, contractors, including private security forces, and suppliers of goods or services. In active or post-conflict settings, non-State armed groups can also pose risks for project critics and have a chilling effect on stakeholders' possibilities to share their concerns. This is particularly the case where such groups have vested interests in the success of a given project, for monetary or other reasons.

At times, PAP may also be divided over the prospect of a development project. In such situations, reprisals within communities or between neighbouring communities can be at issue, and further fuelled by stakeholder engagement with favourable groups or individuals only or by giving project benefits, such as employment, only to those in favour of the project. Typically, however, threats and other forms of reprisals are often seen as emanating from representatives of government: data gathered by the Compliance Advisor Ombudsman, the independent accountability mechanism of the International Finance Corporation (IFC), suggests that in fiscal year 2019, in over 55 percent of retaliation risk cases, complainants reported that threats came from government authorities. In 44 percent of cases, complainants reported threats from the IFC client, while in a few cases only, the source was unknown.<sup>11</sup> Similar data from the Independent Consultation and Investigation Mechanism (MICI) of the Inter-American Development Bank suggests that in the cases handled by the mechanism in 2021, fear of retaliation for engaging with the MICI was expressed by complainants in 55% , including through requests by complainants to keep their identities confidential. The MICI does not disclose the sources of alleged reprisals in annual reporting.

### **ESPF requirements on identifying and managing risks of retaliation**

Through its ESPF, the IDB has committed to an open, transparent, and inclusive engagement process with all stakeholders, including project-affected people, to improve the environmental and social sustainability of the projects it supports. The IDB requires its Borrowers to identify stakeholders potentially affected by and/or interested in IDB-financed projects, and to engage with them in meaningful consultations free of reprisals.<sup>12</sup> The IDB does not tolerate retaliation against those who voice their opinion or opposition to an IDB-financed project or to the Borrower and takes seriously any credible allegations of reprisals.<sup>13</sup>

---

<sup>10</sup> Annex II to the present technical notes provides an illustrative overview of some of the national legal frameworks that may apply in relation to whistle-blower protection.

<sup>11</sup> Annual reporting on incidents in the context of CAO activities (2019).

<sup>12</sup> IDB's commitment to environmental and social sustainability, ESPF (2021).

<sup>13</sup> IDB ESPF (2021), paragraph 7.2.

The ESPF further clarifies IDB's zero-tolerance statement by requiring that Borrowers:

- Undertake a process of consultation with project-affected people and other stakeholders who are subject to identified risks and adverse impacts from a project. This process of consultation should be undertaken in manner that provides opportunities to the project-affected people and other relevant stakeholders, without fear of reprisal, to express their views on project risks, impacts, and mitigation measures, as well as on access to potential opportunities and development benefits, and allows the Borrower to consider and respond to them (*ESPS 1, paragraph 32: Meaningful Consultation and Standard 10, paragraph 21: stakeholder engagement*).
- Put in place workplace processes for project workers to report work situations that they believe are not safe or healthy and to remove themselves from a work situation which they have reasonable justification to believe presents an imminent and serious danger to their life or health... Project workers will not be retaliated against or otherwise subject to reprisal or negative action for such reporting or removal (*ESPS 2, paragraph 28: Occupational Health and Safety*).
- When retaining direct or contracted workers to provide security to safeguard its personnel and property, assess risks posed by its security arrangements to those within and outside the project site. In making such arrangements, the Borrower will make reasonable inquiries to ensure that those providing security are not implicated in past abuses; will train them adequately in the use of force (and where applicable, firearms), and appropriate conduct toward workers and the project-affected people; and will require them to act within the applicable law. The Borrower will not sanction any use of force except when used for preventive and defensive purposes in proportion to the nature and extent of the threat. The Borrower will provide a grievance mechanism for project-affected people to express concerns about the security arrangements and acts of security personnel, and will consider, where appropriate, investigate all allegations of unlawful or abusive acts of security personnel, take action (or urge appropriate parties to take action) to prevent recurrence, and report unlawful and abusive acts to the appropriate public authorities (*ESPS 4, paragraphs 15-17: Security Personnel*).
- Assess and prevent risks of project-related sexual-and gender-based violence and respond promptly and appropriately to incidents such violence and ensure the availability of effective grievance mechanisms that minimize the reporting burden on victims, provide services in a gender-sensitive manner, and minimize reprisal risk (*ESPS 9, paragraph 18: assessing and managing project-related sexual and gender-based violence*).
- Establish a grievance mechanism to receive and facilitate resolution of concerns and grievances about the Borrower's environmental and social performance. The mechanism should seek to resolve concerns promptly, using an understandable and transparent consultative process that is culturally appropriate, readily accessible, in accessible formats, and at no cost



and without retribution to the party that originated the issue or concern (*ESPS 10, paragraph 28: grievance mechanism*).

In addition, the IDB requires its Borrowers to establish processes and procedures within their Environmental and Social Management Systems (ESMS) to monitor and supervise the progress on implementing and achieving the objectives of their environmental and social risk and impact management measures. Borrowers must also comply with all related legal and contractual obligations and regulatory requirements. It is good practice for Borrowers to prepare reports on implementation of projects every 6-12 months and notify the IDB within an agreed number of days if incidents, including incidents that imply allegations of retaliation, have occurred or are imminent. For serious issues, including allegations of serious reprisals, IDB must be notified quickly

### **National laws and policy frameworks requiring identifying and responding to risks of reprisal<sup>14</sup>**

Beyond the retaliation risk requirements expressed in the ESPF, borrowing countries' own legal and policy frameworks may also require the identification of, and appropriate response, to risks of retaliation. Such requirements are typically reflected in laws or policies that address:

- **Access to information, public participation, access to justice and protection of human rights defenders.** The Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean (the Escazú Agreement),<sup>15</sup> entered into force in 2021.<sup>16</sup> Negotiated by governments in Latin America and the Caribbean, it is the region's first environmental treaty with binding provisions on protecting human rights defenders in environmental matters. In 2021, the Agreement had been ratified by 12 countries<sup>17</sup> and signed by 24 countries.<sup>18</sup> It requires signatory States to prevent and investigate attacks against those who protect and defend environmental rights.<sup>19</sup> While State parties are still in the process of transposing the Directive, its provisions on protecting

---

<sup>14</sup> An annex to this publication provides an illustrative list with international agreements and country examples of the types of laws that may be of direct relevance to identifying and managing risks of reprisals, and responding to incidents that have occurred, in relation to IDB projects.

<sup>15</sup> As of August 2021, the Agreement has been ratified by Antigua and Barbuda, Bolivia, Ecuador, Guyana, Nicaragua, Panama, Saint Kitts and Nevis, St. Vincent and the Grenadines, Uruguay, Argentina and Mexico.

<sup>16</sup> Standard 10 in the ESPF (stakeholder engagement) affirms that it is aligned with the principles in the Escazú Agreement, and consistent with the objective of implementing the rights of access to environmental information, public participation in the environmental decision-making process, and access to justice in environmental matters.

<sup>17</sup> Ratification signals the ratifying countries granting approval through their particular political processes and notifying the other parties of their consent to be bound by the provisions of the Agreement. As of January 2022, the 12 countries having ratified the agreement were: Antigua and Barbuda, Argentina, Bolivia, Ecuador, Guyana, Mexico, Nicaragua, Panama, Saint Vincent and the Grenadines, Saint Kitts and Nevis, Saint Lucia and Uruguay.

<sup>18</sup> Signing implies agreement with the terms and expresses the country's intention to comply with the Agreement, however, this expression of intent, in itself, is not binding. In January 2022, the following 24 countries had signed the agreement: Antigua and Barbuda, Argentina, Belize, Bolivia, Brazil, Colombia, Costa Rica, Dominica, Ecuador, Grenada, Guatemala, Guyana, Haiti, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Dominican Republic, Saint Vincent and the Grenadines, Saint Kitts and Nevis, Saint Lucia and Uruguay.

<sup>19</sup> Regional Agreement on Access to Information, Public Participation and Justice in Environmental Matters in Latin America and the Caribbean (2018), article 9.2.

human rights defenders in environmental matters will have important implications for IDB projects, in particular for projects where the safety of environmental defenders may be at issue.

- **Duty to report.** Some of IDB's countries of investment establish a duty on public officials to report criminal acts. Sanctions for those who fail to report, delay or obstruct a report may include a fine, loss of employment, removal from office and disqualification from the exercise of public function.<sup>20</sup> Some jurisdictions classify the failure to report a crime a criminal offence,<sup>21</sup> while others place a general duty to report criminal activity on all people. Such a duty would reasonably apply to reporting forthcoming serious forms of reprisal, for example severe physical violence.
- **Policies, programmes and protection mechanisms for human rights defenders.** Several countries in the region have adopted specific measures for the protection of human rights defenders, such as public policies and programmes. Some countries have also put in place dedicated national protection mechanisms with a mandate to grant protective measures to individuals or groups at particular risk. Such policies, programmes and special measures may have a direct bearing on IDB projects. For example:<sup>22</sup>
  - In 2019, the Ministry of Justice and Human Rights in Peru adopted a protocol guaranteeing the protection of human rights defenders. The protocol is directly binding only on the Directorate General of Human Rights, in the Ministry of Justice and Human Rights and issues eight areas of responsibility for the Directorate General in its work to protect human rights defenders, including designing, implementing, and managing a registry of cases of risk situations for defenders, and setting up an early warning mechanism for timely action by the relevant authorities to respond to attacks or threats against defenders.
  - Colombia's National Protection Unit was established in 2011 under the Ministry of the Interior. The unit has a prevention and protection programme focusing on the rights to life, freedom, physical integrity and security of persons, groups, and communities, which establishes the duty of the State to protect human rights defenders and others through individual and collective prevention and protection measures based on a differentiated and gender-sensitive approach.
  - In 2012, the Mexican Congress passed a federal law to protect human rights defenders and journalists, establishing a national protection mechanism to ensure their life, integrity, freedom, and safety.
  - Brazil established the National Programme for the Protection of Human Rights Defenders in 2004 as the official Brazilian guidelines for protection in cases of threat and risk of life involving individuals, groups or social organizations that act in the defense of human rights and fundamental freedoms. As of 2018, this programme has expanded its mandate to also protect all individuals working as communicators in Brazil including

---

<sup>20</sup> Source <https://www.oecd.org/corruption/Colombia-Phase-3-Report-ENG.pdf> p 56/74.

<sup>21</sup> Source <https://www.oecd.org/daf/anti-bribery/peru-phase-2-report.pdf> p. 13/87

<sup>22</sup> The examples are illustrative only. The list is not exhaustive of protection programmes available to individuals or communities at risk of reprisal in Latin America and the Caribbean.

journalists, bloggers, broadcasters, and media-workers who encounter threats or violence in the course of their work.

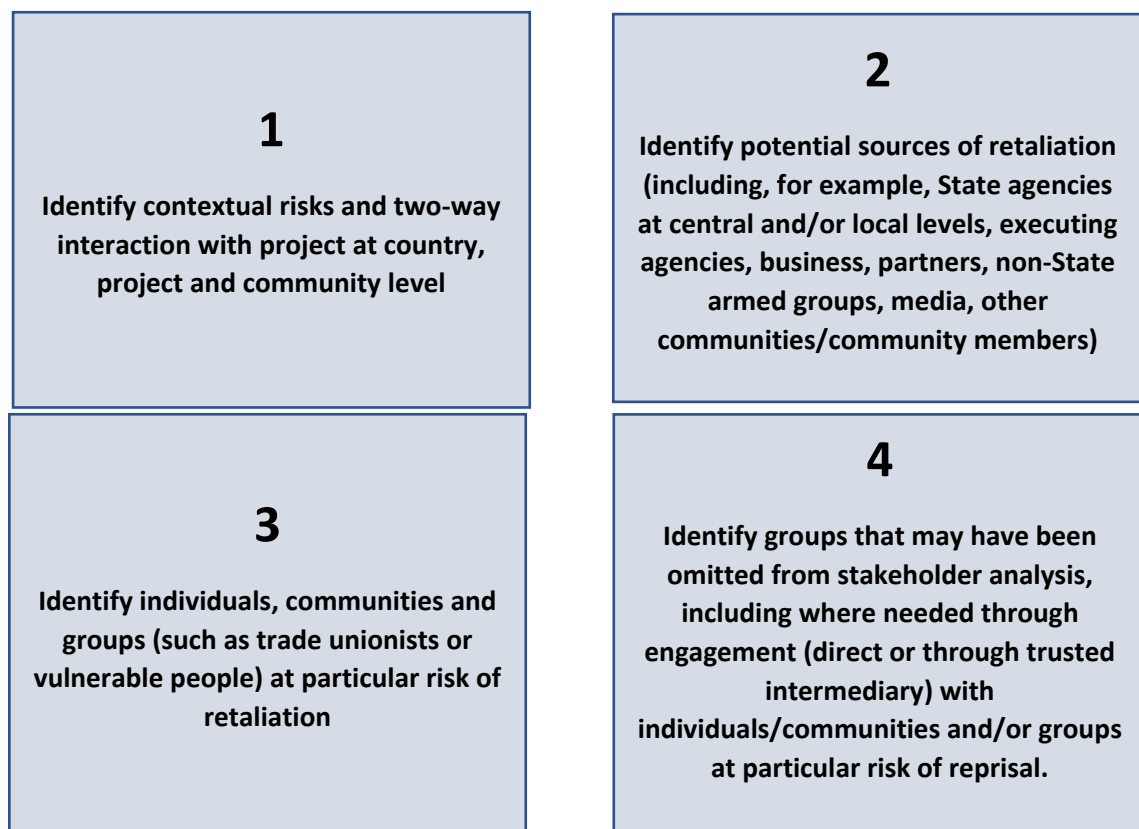
- **Decisions by the Inter-American Commission of Human Rights or the Inter-American Court of Human Rights** may also have direct relevance for an IDB project. This is particularly the case of precautionary measures issued for individuals or communities present in the area where a project is planned or is being implemented. Precautionary measures are urgent requests, directed to an OAS Member State, to take immediate injunctive measures in serious and urgent cases, and whenever necessary to prevent irreparable harm to persons. State compliance with precautionary measures is a requirement: in the event of a history of non-compliance with such measures, the Commission can file a provisional measure request with the Inter-American Court, requesting a legal order for compliance.

## 2. Identify and assess risks of reprisal

The following section supports IDB staff, Borrowers and Executing agencies to proactively identify and evaluate risks of retaliation to project stakeholders, including what types of risks are present in the project area and project area of influence and the two-way interaction between the project and such risks, as well as at-risk individuals and groups and potential sources of retaliation. It recommends a review of available information – both written and through engagement with stakeholders – to determine the overall level of risks and, for the purpose of preparing and implementing stakeholder engagement planes (Executing Agencies) and for evaluating such plans (IDB staff), engagement with individuals and groups that may have been excluded due to their known critical views about the project at issue and/or concerns to their safety.

Contextual risk assessments relating to risks of retaliation are typically done at the earliest stages of project prospecting and design. However, as circumstances change, for example in the event of the emergence of significant tensions around project design, contextual risk assessments should be updated and their findings reflected in project design and implementation, as well as supervision.

*Figure 2. Suggested steps to identify and assess risks of reprisal*



The IDB's ESPF focuses on risk identification, avoidance, and mitigation related to PAP and communities. In contexts where risks of retaliation against project stakeholders runs high, even the best-designed projects can produce unintended consequences. Early identification of risks of reprisal is crucial as it:

- Supports IDB staff to determine the appropriate risk category for projects (with high risk of tension and reprisal correlating with a higher risk category and accompanying due diligence efforts).
- Helps Borrowers and Executing Agencies to design and implement projects in a manner that does not expose project stakeholders to risks of harm by adopting tailored measures to reduce the likelihood that reprisals happen.
- Helps Borrowers and Executing Agencies to be aware of and address material risks in a timely and cost-effective fashion.
- Helps avoid costs and delays in implementation due to unanticipated local protests and project shutdowns.
- Provides IDB and Borrowers with information and knowledge of the situation and allows for better responses to concerns or grievances, including complaints raised through project-level grievance mechanisms or concerns raised with the Bank directly or through accountability mechanisms, such as the IDB's independent accountability mechanism, human rights organisations or courts of law.

### Identifying high-risk projects: contextual risk factors

Retaliation against project stakeholders can be an issue in any project. Some projects, however, will present significantly higher risk than others. Identifying contextual risk factors that increase the likelihood of retaliation is a critical first step for identifying high-risk projects that merit heightened due diligence, including adapted stakeholder engagement plans.

Contextual risk refers to factors that are beyond the direct control of the IDB, but that may have significant impacts on the general security context of a project and on stakeholders' abilities to speak their mind freely. Where contextual factors indicate high risk of retaliation, the mere presence of a project can aggravate existing risks, for example by creating or aggravating rifts between those trying to preserve communal lands and those favouring exploitation of such lands for development purposes.

As has been elaborated in recent guidance by IDB Invest and the International Finance Corporation,<sup>23</sup> common contextual risk factors for retaliation<sup>24</sup> include:

---

<sup>23</sup> [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#). IDB Invest/International Finance Corporation (2021).

<sup>24</sup> The factors presented in this guidance note are not exhaustive, rather they present, in broad strokes, some of the key factors that increase risks at three levels: country, project and community levels. Based on the findings of the contextual risk analysis, additional and more targeted evaluations are typically required to gauge the full extent of risks and the most appropriate ways to address such risks.

- Laws, practice or other circumstances in the country of investment that restrict peoples’ ability to engage freely in public debates and/or deter people from expressing diverging opinions related to Bank-funded project/clients.
- More broadly, risks can also relate to executing agencies and associated business relationships (contractors, sub-contractors, suppliers and consultants) where these have a track-record of taking acts in reprisal against individuals or communities that have sought to express critical views, including in relation to development finance projects.
- At the project level, there are tensions between local authorities/third party actors and other project stakeholders, in particular project-impacted communities, including, but not limited to, over activities linked to the project/investment activities.

At the community level, there are significant divisions between/within, affected communities over impacts and risks associated with the planned project.

The table below provides an overview of key contextual risk factors and suggests potential sources of information to conduct appropriate screening of projects.

**Table 1. Contextual factors that increase risk of retaliation in IDB Projects<sup>25</sup>**

Contextual factors to look for	Suggested sources of information (non-exhaustive)
Ask: what is the quality of civic space, including public participation, at the country level?	
<ul style="list-style-type: none"> <li>• There is little or no active or independent civil society in the country.</li> <li>• There are limited or no protections around freedom of assembly and association (in particular independent trade unions) and collective bargaining.</li> <li>• There are challenges to freedom of the press.</li> <li>• There have been past instances of retaliation against individuals or groups in the country.</li> </ul>	<p>The <a href="#">CIVICUS Monitor</a> tracks, on an ongoing basis, the state of civic space in all countries of the world and provides rankings for each. It also includes information on reprisals that have taken place in each country.</p> <p>The <a href="#">World Governance Indicators</a> reports aggregate and individual governance indicators for over 200 countries and territories over the period 1996–2020, including in relation to Voice/Accountability and Violence/Terrorism.</p> <p><a href="#">ITUC’s global rights index</a> provides an overview of the state of trade union rights by country. The index is updated annually.</p> <p><a href="#">Reporters Without Borders’ World Press Freedom Index</a> ranks 180 countries and regions according to the level of freedom available to journalists. It is a snapshot of the media freedom situation based on an evaluation of pluralism, independence of the media, quality of legislative framework and safety of journalists in each country and region. <a href="#">Freedom House</a> assesses the challenges for media and online freedom in its annual <i>Freedom and the Media</i></p>

<sup>25</sup> Adapted from [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#). IDB Invest/International Finance Corporation (2021).

Contextual factors to look for	Suggested sources of information (non-exhaustive)
	<p>and <i>Freedom on the Net</i> reports and provides scores for each by country.</p> <p>The <a href="#">Inter-American Commission for Human Rights</a> provides information on retaliation against local activists in its member countries, including through <a href="#">press statements</a>, <a href="#">country reports</a> and <a href="#">precautionary measures</a> in favour of individuals or groups under threat. The Commission has a dedicated Rapporteur on the situation of human rights defenders in the region.</p> <p>The <a href="#">UN Special Rapporteur on Human Rights Defenders</a> has a global mandate and addresses the situation of individuals and groups that, because of the work they do, are referred to as human rights defenders. The Rapporteur produces <a href="#">country reports</a> and <a href="#">communications</a> with State authorities.</p> <p><a href="#">Protectdefenders.eu</a> has an index of alerts that provides information on reprisals against individuals by country, type of reprisal and profile of the victim (thematic area of work, profession and gender).</p> <p>The <b>UN Secretary General</b> releases <a href="#">annual reports</a> that document and analyse available information on alleged intimidation and reprisals against individuals or groups for cooperation with the UN, its representatives and mechanisms in the field of human rights. The UN Assistant Secretary-General for Human Rights has been designated to lead the efforts within the UN system to address the issue.</p>
<p>Ask: do executing agencies and/or associated business relationships that will have a role to play in the design or implementation of the project have a track-record of retaliating against individuals or groups that have sought to peacefully express critical view?</p>	
<ul style="list-style-type: none"> <li>• Executing agencies have, in the past, been known to retaliate against local activists or organisations or have expressed their intent to punish such individuals or groups if they express their views to the Bank or in public.</li> <li>• There is information to suggest that business relationships</li> </ul>	<p>Relevant documents and information provided by the client, in particular health and safety records, notices of material labor issues between management and workforce / workforce- external stakeholders (i.e., strikes, demonstrations, security incidents), poor security management records from previous projects, and material community grievances and high-profile adverse press reports on E&amp;S matters.</p> <p>For information on past instances of retaliation, the Business and Human Rights Resource Centre <a href="#">database</a> provides up-to-date</p>



Contextual factors to look for	Suggested sources of information (non-exhaustive)
<p>(contractors, sub-contractors, suppliers or consultants) have a history of tension and distrust with communities or groups in the project area / area of influence.</p>	<p>information on allegations of retaliation by individual companies and company responses to these allegations.  E&amp;S intelligence systems, such as RepRisk, that rely on artificial intelligence to compile a large amount of online news, campaigns and reports addressing a pre-defined list of E&amp;S risk topics, and prepares analysis and summaries of these findings per region and client, amongst others.  National human rights institutions.  <a href="#">UN Human Rights Office through relevant field presences.</a>  Research using local media and web resources.  Information gathered in the context of IDB site visits.</p>
<p>Ask: is there tension in the project area / area of influence?</p>	
<ul style="list-style-type: none"> <li>• There is a history of tension between local authorities and communities in the area, including in relation to land ownership and usage.<sup>26</sup></li> <li>• There have been past instances of retaliation in the area. Communities or individuals in the area have voiced opposition to development projects.</li> <li>• Vulnerable groups with high levels of social inequality and disempowerment are present in the project area.<sup>27</sup></li> </ul>	<p>Through its <a href="#">field presences</a>, the <b>UN Human Rights Office</b> provides regular reporting on the situation in a number of countries. Field presences are increasingly being mobilised to monitor situations in specific regions as they relate to private sector investment and can provide additional information on the situation on the ground.  The <a href="#">Heidelberg Institute for International Conflict Research</a> provides, through its annual Conflict Barometer, an overview of the emergence, dynamics and settlement of political conflicts worldwide. <a href="#">International Crisis Group</a> maintains a live global conflict tracker with developments in over 80 conflicts and crisis.  <a href="#">National Human Rights Institutions</a> through ongoing monitoring and reporting, can provide additional information on the situation in specific regions.</p>

<sup>26</sup> Legacy land issues are major red flags for contextual risk of conflict and retaliation. Legacy land issues tied to an investment frequently result from i) historically unresolved claims to land; ii) the type and level of community consultation and consent process prior to a land acquisition; iii) the terms and processes for land acquisition and compensation; iv) poorly applied resettlement procedures; v) restricted access to land by communities, including seasonal users like pastoralists or community members with overlooked land rights; and vi) the extent of land use by the project operator. See [https://uploads-ssl.webflow.com/5d819417269ec7897f93e67a/5dcb5578c74abf5dc2f80f18\\_Interlaken\\_Group\\_Land\\_Legacy\\_Guidance.pdf](https://uploads-ssl.webflow.com/5d819417269ec7897f93e67a/5dcb5578c74abf5dc2f80f18_Interlaken_Group_Land_Legacy_Guidance.pdf)

<sup>27</sup> The socio-economic inequality directly correlated with power imbalances that can have profound roots in societies and possibly be reflected in the scenario of any development project in the region. Social inequality and disempowerment will mostly affect the most vulnerable communities, making them more susceptible to reprisals



Contextual factors to look for	Suggested sources of information (non-exhaustive)
<ul style="list-style-type: none"> <li>Individuals or communities in the area are subject to precautionary measures due to legitimate concerns to their safety.</li> <li>There is active or latent conflict in the area. Public or private security forces or armed groups may be present.</li> </ul>	<p>The <a href="#">Inter-American Commission for Human Rights</a> provides information on <a href="#">precautionary measures</a> in favour of individuals or groups under threat in specific countries and localities in IDB's regions of investment.</p> <p>Project stakeholders, including local/national/international civil society organisations or community-based organisations that have information about the situation in the project area.</p> <p>Local and international news agencies.</p>
<p>Ask: is there conflict within or between project-impacted communities?</p>	
<ul style="list-style-type: none"> <li>There is significant tension between, or within, PAP over the project.</li> <li>There are groups within the PAP community/communities that are marginalized (such as, for example, women) and that are likely to be excluded from decision-making processes.</li> </ul>	<p>Project stakeholders, including local/national/international civil society organisations or community-based organisations may have information about the situation in the project area.</p>

A key purpose of a contextual risk identification and assessment is to capture how a project will interact with contextual risk factors. Such interaction, or linkage, can be addressed by considering, in relation to the contextual risk factors identified, issues such as:

- How does this factor interact with planned or ongoing project activities?
- What kinds of risks (of retaliation) could the contextual factor pose for planned activities and services that are provided by the project? In particular, what challenges could the contextual risk factors pose for meeting IDB ESPF requirements relating to inclusive stakeholder engagement that is free of retribution?
- Based on identified factors, are there particular groups that may be at higher risk of retaliation than others (such as indigenous community leaders, trade unionists, members of campesino communities or afro-descendants, women etc.)? Are such groups present in the project area / area of influence and, if so, have these groups voiced concerns over the planned project or other similar projects in the past?

---

and repression if and when raising concerns. A proper mapping of these vulnerable groups, their decision-making process and existing power imbalances are key as overall contextual risk components as a preventive tool.

- What are the common sources of threat (perpetrators of retaliation) and what role may these have in project design/implementation? What influence will they have over project activities (e.g., the agencies that have the overall responsibilities for conducting stakeholder mapping and/or consultation processes have conflictual relationships with PAPs and/or have been known to exclude critical voices in the past)?

In summary, screening projects for contextual risk should support the identification of the level of risk, the potential perpetrators and victims of retaliation and the form and severity that retaliation may take, should the risks materialize. It should also be a starting point for thinking about how to plan and conduct stakeholder engagement in a way that does not expose project-impacted communities and others associated with them to harm for seeking to express opposition or critical views, and to design, in collaboration with those at risk, measures needed to prevent or mitigate such risks as well as potential responses should risks materialise

### **Stakeholder identification and analysis: identifying stakeholders that risk being omitted due to critical views and/or concerns to their safety**

Beyond identifying which projects may be risky from a reprisals point of view, a contextual risk assessment should also assist to identify any individuals and/or groups that risk being omitted from stakeholder engagement processes if they have expressed, or if it is perceived that they will, express opposition or critical views and perceived concerns over their own or their families' safety. In particular, a screening for project level tensions should inform strategies for the inclusion of such groups in stakeholder engagement plans and associated processes in a manner that does not expose them to harms for sharing their views. Depending on circumstances, for example where there are significant tensions between local authorities and PAPs, third-party specialists can also be retained to assist in such stakeholder identification and analysis and to support the design of an inclusive engagement process. Where third parties are engaged, these should have the appropriate level of expertise in working with groups subject to repression and implementing corresponding safety measures when engaging with such groups.

### 3. Prevent or mitigate risks of reprisal

The following section highlights some of the key measures that the IDB, Borrowers and Executing Agencies can take to address risks of retaliation as part of project design, implementation, monitoring and closure. It highlights the importance of:

1. Proactively communicating IDB's zero-tolerance to reprisals to all project stakeholders, including Borrowers, Executing Agencies and business relationships with a key role in project design and implementation (contractors, sub-contractors, suppliers and consultants) PAP individuals and communities.
2. Building capacity among Borrowers and project implementing agencies and their staff to identify and address risks of retaliation, including in the context of designing inclusive stakeholder engagement plans and running effective operational level grievance mechanisms.
3. The need to adapt disclosure of information practices to prevent/mitigate risks of retaliation based on the recognition that requesting that participants at consultation processes be required to disclose their identities and that this is shared may expose them to significant risk of retaliation or exacerbate existing risk.
4. Planning consultation processes, both in person and online, in a way that does not expose participants to risks.
5. Considering the possibility to request the support of independent third parties to defuse tensions and reduce the likelihood that reprisals materialise.
6. IDB conducting additional stakeholder engagement without the involvement of the Borrower and/or executing agencies in given circumstances.
7. Designing operational level grievance mechanisms in a way that does not expose complainants and others associated with them or with the complaints handling process to risks of retaliation and communicating to project stakeholders that they retain the right to approach the IDB's independent consultation and investigation mechanism directly if there are concerns relating to safety.
8. Ensuring that those working on the project - whether at the Bank or Borrower/Executing agency-level have the right set of skills to handle risks to retaliation and that, where retaliation risks are high, staff turnover be limited to ensure a coherent institutional memory about risk mitigation measures and responses to reprisals that have been agreed.
9. Understanding the role of IDB's independent consultation and investigation mechanism in responding to requests from PAP including in relation to risks of reprisal.

Through its ESPF, the IDB requires Borrowers to identify stakeholders potentially affected by and/or interested in IDB-financed projects, and to engage with them in meaningful consultations free of reprisals. Clients are required to develop and

implement a stakeholder engagement plan that is proportionate to the nature and scale of the project and its potential risks and impacts, commensurate with the project-level circumstances for stakeholder engagement. The plan should describe the timing and methods of engagement with stakeholders throughout the project life cycle, distinguishing between affected stakeholders and other stakeholders. It should also describe the range and timing of information to be communicated, as well as the type of information to be sought from affected stakeholders and other stakeholders.

### Communicating zero-tolerance and building capacity<sup>28</sup>

An important measure to address risks is an early conversation with project partners, including Borrowers and Executing Agencies but also suppliers, contractors (such as security forces) and consultants that may have a key role to play in project design, implementation and monitoring.

Communicating the Bank's zero-tolerance, as expressed in the ESPF, is necessary to be able to set a common understanding of potential risks of retaliation against project stakeholders and the need to address such risks in an appropriate manner. An early discussion sets the expectation clearly that retaliation will not be tolerated, and the project-specific measures may be needed to identify the risk that actors associated with a project. When engaging on the topic of retaliation, it may be worthwhile to:

- **Choose appropriate language.** Retaliation is a sensitive issue and raising it directly as such can be tricky. Contextual risks can be an important entry point to a discussion about retaliation risks (such as, for example, the use of certain laws to incarcerate local activists), as can raising examples of potential measures to address specific issues (such as, for example, ensuring confidentiality of complainants to operational-level grievance mechanisms).
- **Reach agreement on how zero-tolerance expectation will be communicated to key business partners** such as executing agencies, suppliers or contractors. For example, Borrowers can commit to communicate zero-tolerance to retaliation through formal agreements or documentation (for example through supplier codes of conduct) that include:
  - Expectations on the behaviour of direct and subcontracted employees when outside work and inside host communities.
  - Reporting requirements addressing any allegations of retaliation and how those have been resolved.
  - A commitment to resolve any disputes that may arise through dialogue-based means.
  - Specification about whether/how the business relationships are expected to cascade requirements to their own business relationships.

---

<sup>28</sup> Adapted from [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#). IDB Invest/International Finance Corporation (2021).

- Grounds for terminating contracts due to failure to meet the zero-tolerance commitment.
- **Adopt an “if in doubt, tell” approach:** project partners, including Borrowers and Executing Agencies, should be encouraged to communicate any concerns they may have around for example community opposition to projects and any associated security incidents.
- **Raise the possibility that stakeholder engagement plans may need to be adjusted over the course of the project:** project partners, including Borrowers and Executing Agencies, should be alerted to the fact in Providing for the possibility of policy adjustments in relation to stakeholder engagement in the event in case existing plans are not responding to the needs of the project or when unexpected circumstances arise during project implementation that may give rise to retaliation.

The best protection from retaliation that IDB, Borrowers and Executing Agencies can provide to PAP individuals and communities is to be aware of potential risks of harm and to exercise good judgement, caution and sensitivity toward these risks in all their interactions. An important component of an effective strategy to address risks of retaliation is therefore capacity-building, not only within IDB but also with Borrowers and Executing Agencies.

Building capacity is an important measure to create a bottom-up culture that emphasizes the importance of an open feedback culture and to ensure that potential allegations of retaliation can be dealt with in a manner that does not expose victims to further risks. The key is to involve staff across a wide range of functions, as managing risks of retaliation is likely to involve a number of teams and agencies. In particular, investing in capacity-building on the ground staff (whether working for the executing agency or associated business relationships with a key role in project design or implementation) is essential as they will have direct and ongoing engagement with project stakeholders and may be faced with situations where risks, or allegations of, retaliation emerge.

The following questions can be useful to consider when designing targeted capacity-building:

- Whose capacity do we need to build? What agencies or project partners would benefit from such training and what level of decision-making?<sup>29</sup> Which project workers will play an important role to manage risks (e.g., security guards, other contractors with daily interaction with project stakeholders, staff receiving and responding to potential complaints from project-impacted communities) and that could be involved in training? Should specific training be offered to those in charge of operational-level grievance

---

<sup>29</sup> For example, managers, and high management officials including decision-makers at different levels could benefit from training sessions on reprisals and reprisals risk management as a means to reflect upon how addressing stakeholder concerns, as a way to defuse tensions and reduce risks of retaliation, may impact project implementation timelines. Experience from DFI projects with reprisals have shown that pressure to meet project timelines may result in actions that amount to coercion and retaliation perpetrated by lower-rank workers.

mechanisms, to ensure the safe handling of complaints (such the safe storage of information, ensuring confidentiality)?

- What should the training cover? Common elements of retaliation risk management training include:
  - What is retaliation? What acts constitute retaliation? Who may target project stakeholders and how? Why is it important to manage risks of retaliation?
  - What are some of the common risks of retaliation at the country/project level (and project level of influence/community level) and how does the project interact with these risks (e.g., by planned operations in an industry where the Borrower country has established (i) restrictions on forming independent trade unions, (ii) business cultures and attitudes that are hostile to trade union rights, (iii) laws that restrict the work of civil society organisations, or (iv) an increase in criminalization of local activists)?
  - How can retaliation impact members of the project workforce and how can it affect PAPs? Are there groups that, based on the sectors in which we operate, seem to be at particular risk?
  - What are some of the practical measures that have been taken or that could be taken to manage these risks? What are some of the options available for responding to potential incidents (of retaliation), who should be informed and be responsible for follow-up and how should incidents be communicated to IDB?
- When would be the ideal time for organising training and in what format? For example, in the context of corporate training for project workers, or when onboarding new company staff in key functions? Could stand-alone training on specific issues, such as conflict-resolution, be considered, or would including discussions on retaliation into existing training be a better option?
- Who should deliver the capacity-building? Could training be done by in-house staff or could external resource organisations with relevant local or thematic (e.g., trade union rights, civic space) expertise have a role to play? Could national human rights commissions have a role to play, or protection programmes for human rights defenders if these exist at the national level? Are there contexts where international expertise is needed, both to protect the welfare of the trainers who themselves could face retaliation, and to assure that the trainers can speak freely?

### Planning inclusive stakeholder engagement

As indicated above, certain groups and individuals may, due to concerns to their safety, self-censor, or because they have expressed critical views, find themselves excluded from stakeholder engagement processes for having expressed opposition to, or concerns over, projects funded by the IDB. Such groups are often labelled anti-development or troublemakers and are at risk of reprisal.

Excluding group with critical views from stakeholder engagement plans or ignoring their concerns is likely to fuel additional tensions, resulting in local protests and

shutdowns with material impacts on the success of the project. Maintaining an ongoing dialogue throughout the project cycle that demonstrates responsiveness to stakeholder concerns, to the project broadly and in addition in relation to their security situation is an important means to defuse conflict, and reduce risks for confrontation and retaliation.

The IDB expects that Borrowers seek the views on project-associated risks and impacts from a broad range of stakeholders, including those who are the most vulnerable to adverse impacts and those who are critical against, or oppose, the project, to ensure that project risks and impacts are known and can be appropriately addressed. A good stakeholder engagement plan therefore identifies a broad range of stakeholders, including critical such, and seeks to engage these in meaningful consultation at various steps of project design, implementation and monitoring.

Any stakeholder engagement plans, and associated consultation processes, should also be designed in a way that does not expose groups or individuals at risk of harm for exercising their right to express their views. In particular, the 'safe' aspect of stakeholder engagement entails designing and implementing specific protection measures to ensure that stakeholders can freely express their opposition to projects or otherwise express concerns. As the section below indicates, depending on the potential source of reprisals as identified by those at risk, this may necessitate one-on-one conversations off-site of project operations, in locations selected by stakeholders. In others it may involve strict protocols that exclude management, security, or other personnel that are seen as posing risks of retaliation from participating in or having access to participant lists from discussions.

### **Adapting disclosure of information requirements where risks of retaliation are at issue**

The ESPF underscores the importance of the Borrowers disclosing project information that allows stakeholders to understand project risks, impacts, and potential opportunities and development benefits. The Borrower is expected to provide access to information as early as possible in the project development process, and within a timeframe that enables meaningful consultations with stakeholders on project design. As is specified in ESPF 10, amongst others, the information to be disclosed includes:

- a description of the area of influence and physical and technical characteristics of the proposed project or activity
- the duration of the proposed project activities
- potential risks and impacts on local communities and the environment and proposals for mitigation
- potential opportunities and development benefits, and
- the proposed stakeholder engagement process, including
  - ways in which stakeholders can participate,



- the time and venue of any proposed public consultation meetings and the process by which meetings will be notified, summarized, and reported, and
- the process and means by which grievances can be raised and will be addressed.

Where risks of retaliation are at issue, for example where some stakeholder groups gave signalled concerns to their safety for expressing their views, the public information requirements relating to the stakeholder engagement process may need to be adapted. For example, dedicated consultation events with individuals or groups at risk, or the timing and venues for such consultations, should not be disclosed as doing so may lead to unwelcome intruders at such meetings, and increase the likelihood that participants are subject to reprisal. Similarly, redactions on any reporting on consultation meetings may need to be done, such as blackening out participants names' or anonymizing the source of critical views. The specificities of such redactions will need to be agreed with participants, although a note on the possibility to do so could be included in any publicly displayed information on consultation meetings. As a general rule, participants' names should not be publicly disclosed and if they give their name during the consultation, for example for purposes of signing attendance sheets, then they should be informed about how such information will be used and be given the option of not having their names disclosed.

Where physical access is restricted or stakeholders are unwilling to participate in physical meetings due to concerns to their safety, electronic communication channels can serve as a useful way to engage. Virtual consultations, however, carry their own risks for potential reprisals, in particular if parties external to the consultation can easily enter the virtual meeting, if it becomes known who has attended the consultation or if external parties get access to the meeting materials, including minutes and lists of participants. A number of measures can be considered to reduce the risk that confidentiality of participants cannot be maintained. An important measure is to devote time to identify the best – from a digital safety point of view<sup>30</sup>– communication platform or conferencing tool to be used, rather than to automatically rely on the common platforms that are already being used by the organisation. Platforms that ensure end-to-end encryption should be prioritised as this permits any messages to be encrypted before leaving a device and remaining encrypted until it reaches the intended recipient's or recipients' device. Using end-to-end encryption is important if sensitive communication, such as during internal team or partners meetings, will be shared. Some additional questions<sup>31</sup> to consider when choosing the conferencing tool include:

---

<sup>30</sup> The following section draws on Front Line Defenders, April 2021. Guide to Secure Group Chat and Conferencing Tools, available at <https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools>

<sup>31</sup> Front Line Defenders, April 2021. Guide to Secure Group Chat and Conferencing Tools, available at <https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools>



- Does the platform provide encryption? Is it end-to-end encrypted or just to-server encrypted?<sup>32</sup>
- How do you connect with others?
- Is the virtual room password protected? Who has access to the password?
- Do you need to provide phone numbers, emails or nicknames during the call or can participants remain anonymous?
- Do you need to install a dedicated app/program?
- What will this app/program have access to on your device (address book, location, mic, camera, etc.)?

It should be noted that choosing communication platforms solely based on security considerations may not always be optimal, in particular if the intended participants in a confidential meeting have limited connectivity and/or experience of using only communication platforms or online conferencing tools. This is a particular concern for highly marginalized stakeholders and for older stakeholders, both of whom may have critical perspective on the topic of reprisal risks. Therefore, a balance must often be struck between digital security and accessibility. To make an informed decision about how to best strike this balance, it is recommended that digital security experts, ideally with expertise on the country or region concerned, are consulted, and that the views of the intended participants are also taken into account.

During the online consultation itself it is considered best practice<sup>33</sup> to make sure that you know who is connected: this can be done by checking the identities of the participants by asking them to speak. Additional best practice to ensure safety also includes agreeing on ground-rules during the call, this would typically entail raising and agreeing on issues like keeping cameras on/off, keeping microphone on/off when one is not speaking, who will be chairing the meeting, who will take notes and where and how will those notes be written and then distributed, and whether screenshots can be taken during a video call, and if the call can be recorded or not. Ahead of the consultation, participants should be warned about any potential vulnerabilities such as, for example, if the platform is not encrypted or if the meeting will be recorded. Where they are fearful of a risk of retaliation participants should be encouraged to log in using a pseudonym. To address security risks, coordinators of online consultations can also opt for establishing an 'unsafe word' that participants could use in the event they experience surveillance (e.g., a visit by security forces) during the consultation (to be dropped from the call) and a 'safe word' that can be spoken to be let back into the online consultation meeting.

---

<sup>32</sup> With encryption to-server, the message is not encrypted for its entire journey. It is encrypted before it leaves the device, but the service that is used (like Google Meet or Microsoft Teams) decrypts it for processing and re-encrypts it again before sending to recipient(s). That means someone who has access to servers could potentially intercept the message. Having encryption to-server is typically fine as long as the server can be trusted. For more information see Front Line Defenders, April 2021. Guide to Secure Group Chat and Conferencing Tools, available at <https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools>

<sup>33</sup> Front Line Defenders, April 2021. Guide to Secure Group Chat and Conferencing Tools, available at <https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools>

Beyond sharing information about the project and its perceived risks and impacts, and as indicated above, it is advised that project stakeholders are informed of IDB's zero-tolerance to reprisals. Pro-actively communicating zero-tolerance to retaliation to project stakeholders is in itself an important measure to reduce risks of reprisal: where the expectation has been communicated clearly, potential perpetrators are typically less likely to commit acts in reprisal out of concern for consequences for doing so, and impacted stakeholders more likely to report any such incidents. Setting the expectation clearly at the outset that IDB values the feedback of all stakeholders, also those with critical views and that reprisal will not be tolerated, sets an important foundation for working with parties to address such risks throughout project design, implementation and monitoring.

The ESPF also requires Borrowers to inform project-affected people about the project's grievance mechanism and the IDB's independent accountability mechanism for project affected people in the course of the stakeholder engagement process. In this regard, highlighting the MICI's recently adopted retaliation risk management guidelines is advisable, as is the fact that where stakeholders fear reprisal for engaging with project partners, they are free to submit such concerns directly to the MICI confidentially, without any prior communication of such concerns to the IDB management.

Lastly, the use of photos of participants to consultations in public-facing reports or outreach material can pose significant risks of future reprisals to those that appear in the pictures.<sup>34</sup> Images should never be taken without their express consent, and identifiable images of individuals with confidentiality protection, or indications of their locations, should not be included in documenting aspects the consultation process through photographs, without their express consent for doing so. Photos of parties should only be used for publication purposes when appropriate permissions have been sought and the parties are aware how the images will be used. Notwithstanding if consent has been obtained for the use of photographs, the value and importance of using photos should be carefully weighed against the possible risks of future reprisal against the photographic subject. If there is a risk of harm, information (including photos) should not be disclosed.

### **Conducting meaningful consultation with due consideration for security concerns to participants<sup>35</sup>**

The IDB requires Borrowers to undertake a process of meaningful consultation in a manner that provides opportunities to project-affected people and other relevant stakeholders, without fear of reprisal, to express their views on project risks, impacts, and mitigation measures, and on access to potential opportunities and development benefits, and allows the Borrower to consider and respond

---

<sup>34</sup> Office of the UN High Commissioner for Human Rights. Manual on Human Rights Monitoring, [Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons](#); Inter-American Development Bank: Independent Consultation and Investigation Mechanism, 2019. [Guide for Independent Accountability Mechanisms on Measures to Address the Risk of Reprisal in Complaint Management](#).

<sup>35</sup> This section draws on [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#). IDB Invest/International Finance Corporation (2021).

to them. Borrowers should carry out meaningful consultation on an ongoing basis to an extent and degree that is commensurate with the project's risks and adverse impacts and with the concerns raised by project-affected people and other relevant stakeholders.

When conducting such consultations, Borrowers should be mindful that some stakeholders may either feel reluctant to attend, due to fear of reprisal for doing so, or may be unaware of such risks or accept them and be subject to retaliation by others for having participated.

Where the Borrower conducts the consultations, such risks should be taken into account when designing and executing the consultation processes. For example, where physical meetings will be held, it may be worthwhile to consider:

- **Organising dedicated meetings:** should dedicated meetings be held with groups at risk of reprisal? If so, how could these groups be approached?
- **Raising security concerns:** are stakeholders aware of the risks that participation can entail? If not, how can potential concerns over safety best be raised with participants in advance?
- **Who will organize and run the consultation(s):** where, for example, there are tensions with project stakeholders, could an independent third party be brought in to conduct consultations, e.g., a national human rights commission or other actor that enjoys the trust of stakeholders?
- **Location:** where could the consultation(s) be held? Are there locations that the participants prefer to reduce potential risks that they are under surveillance (e.g., in a neighbouring village in the project area, in the capital of the country, at places of religious worship etc.)?
- **Anonymity:** will names of participants be collected and if so, how will these be stored? Could the 'Chatham House' rule be applied (where views are documented and may be made public, but not attributed to specific individuals or groups)?
- **Confidentiality of information:** will meeting notes be taken and how will these be used (e.g., communicated to a select number of staff, other project partners, or made public)?
- **Electronic devices:** has the potential for surveillance been flagged and agreements established about when and where it is acceptable to store and use electronic devices? Where there are security concerns, has agreement been reached on whether, and how, information about the consultation can be posted on social media?
- **Sharing security contacts:** have participants been informed that they can share information about something that is out of the ordinary (e.g., potential surveillance of the consultation) and have participants been provided with contact information to communicate potential incidents arising after the meeting?

While these questions will be relevant for any stakeholder consultation, they are all the more important in contexts where stakeholder groups have expressed fear of retaliation for their participation in consultation processes. Where this is the case, organising dedicated and closed-door meetings with such groups is particularly important to ensure that they can freely share their concerns.

In terms of content, stakeholder consultation meetings, whether stand-alone with groups at risk or general, could seek to establish:

- **If there are particular concerns or fear that people will be punished for having expressed critical views.** Proactive engagement with stakeholders over risks of retaliation not only helps to develop the risk picture for a project but is also an important means to communicate to stakeholders that all feedback – positive or negative – is welcome, that retaliation will not be tolerated and that any allegations of retaliation will be addressed.
- **How potential risks could be addressed, in particular in terms of design and implementation of grievance mechanisms.** For example, would stakeholders prefer to communicate through third parties, so as to ensure their anonymity? Are there already local protection strategies in place at the individual and/or communal level, and how could these types of strategies be supported?
- **In the event of particular security incidents that amount to reprisal or create favourable conditions for reprisals to occur, what would appropriate responses be and who should be contacted?** Agreeing on measures to be taken in the event of reprisal is paramount before the reprisal happens as individuals at risk may have been made to go missing or gone into hiding and can no longer be reached as a result of an imminent threat or reprisal.

### Working with independent third parties

Conflictual relationships between project partners and project stakeholders increase the risk of confrontation and potential acts of retaliation. Addressing the issues and concerns that underpin such conflictual relationships is an important means to defuse conflict and reduce the likelihood that retaliatory acts in response to protests or other forms of local opposition. Where relationships are strained and direct dialogue between project implementing partners and stakeholders is challenged, retaining external neutral and independent third parties may be a means to build constructive engagement. While neutral third parties are typically only brought into the project where concerns have been raised with the Bank's independent consultation and investigation mechanism, engaging mediators or conciliators at the earliest stages of project design could support a more constructive engagement and open dialogue throughout the lifespan of the project.

When project stakeholders are unwilling to participate in public or dedicated consultations due to security or other concerns, interlocutors such as civil society organisations, trade unions, national human rights institutions or relevant international organisations with presence in the country concerned can also be

mobilised to act as intermediaries to convey any potential concerns related to risks of retaliation or to the project more broadly. A list of organisations that could provide such assistance is included in an Annex to the present note. It should be noted, however, that these organisations may not be available to support identified risk mitigation measures, including as intermediaries conveying concerns.

### **Where stakeholder engagement is the responsibility of a government agency not in charge of project implementation**

The ESPF highlights that where stakeholder engagement is the responsibility of a government agency that is not involved in project implementation, the Borrower will collaborate with the responsible government agency to achieve outcomes that meet the objectives of this ESPS. In addition, where necessary, the Borrower will play an active role during the stakeholder engagement planning, implementation, and monitoring process to support the achievements of the objectives of this ESPS.

At times, government agencies in charge of consultative processes may have a conflictual relationship with project stakeholders or has limited experience of conducting stakeholder engagement in contexts where guaranteeing the security of participants is a challenge. In these kinds of situation, it may be worthwhile to engage with the responsible government agencies and raise concerns over potential retaliation. It should be noted, however, that retaliation is a sensitive issue and raising it can be tricky. Where this is the case, contextual risks can be an important entry point to a discussion about retaliation risks (such as, for example, the use of certain laws to incarcerate activists), as can raising examples of potential measures to address specific issues (such as, for example, ensuring confidentiality of complainants to operational-level grievance mechanisms). Reaching agreement on how zero-tolerance to reprisals will be communicated to project stakeholders – both partners and impacted communities – can also be an important way to bring the issue into the spotlight. Lastly, agencies in charge of consultation should be encouraged to communicate any concerns they have around community opposition to projects and any associated incidents.

The ESPF also highlights that if the process conducted by a government agency not involved in project implementation does not meet the relevant requirements of this ESPS, the Borrower will conduct a complementary process and where appropriate, identify supplemental actions.

In other words, additional verification of previously conducted stakeholder engagement may be required. This is in particular the case where stakeholder engagement plans seemingly omit marginalized and discriminated against groups, and/or only indicate that feedback has been positive, despite publicly available information that there is tension and opposition to the project in question in the area. Verification of stakeholder engagement can include retaining third-party independent experts to review records of stakeholder mapping, engagement strategies, and records of stakeholder engagement processes that have concluded to determine whether these have been inclusive, adequate and free of intimidation and threats, and what actions could be taken to address such concerns. Where reviewing such documents and processes is considered needed, third parties such as civil society organisations or trade unions with local presence or expertise, for

example, could serve useful to act as intermediaries and provide information about potential concerns that may have been overlooked due to safety concerns.

### **Additional stakeholder engagement by IDB**

While stakeholder engagement is typically the responsibility of the Borrower, it may be prudent for IDB to conduct independent consultations with project stakeholders where risks of retaliation are at issue. Where a contextual risk screening identifies high-risk contexts, IDB can heighten scrutiny of stakeholder engagement plans and identify additional needs for stakeholder engagement. Where this is the case, the focus should be on identifying and engaging with particular groups that may not have been accurately identified as stakeholders and not participated in consultation processes out of fear of retaliation for expressing their views, or have already been threatened by key project implementing partners to not express their views. In these types of circumstances, IDB retains the right to conduct additional stakeholder engagement with the support of stakeholder engagement specialists within the Bank and, as will typically be the case in these types of circumstances, by independent third parties with expertise in safe engagement with individuals or communities at high risk of reprisal.

A number of red flags can demonstrate the need for confidential, IDB-led consultations, such as, for example:

- Lack of representation from members of affected communities (some communities, or all communities)
- Presence of security forces at consultations
- The manner in which project partners speak about project stakeholders (for example, as troublemakers, anti-development, terrorists)
- The imposing presence of some project partners at consultations
- That project-impacted stakeholders express views during bilateral talks, but few, if no one, express their views in context of public consultations,
- Clear favouritism of some community members, or some communities, that appear to be favouring the project or specific project activities subject to consultation.

Past experience suggests that where institutional investors have taken on a role of conducting additional stakeholder engagement, structured engagement with stakeholders has at times been subject to participation of representatives from government agencies with a strained relationship with the interviewees. This type of situation can be handled by simply insisting, as a requirement of Bank assistance, that their representatives be allowed to carry out independent, confidential community surveys and that it is IDB procedure that all such interviews have to be confidential.

Where the Bank conducts independent consultations, it is important to emphasize to stakeholders that Bank staff do not represent project implementing authorities and that any information that is disclosed will not be directly communicated – with names and personal information, for example – to the Borrowers or other parties associated with the project. In addition, carefully choosing interpreters where needed will be an important aspect of how to design and implement independent consultations: interpreters should be independent and neutral and not associated with Government and/or Executing Agencies.

### Organisational capacity and commitment

The ESPF requires the Borrower to define clear roles, responsibilities and authority and to designate specific human and financial resources to be responsible for the implementation and monitoring of stakeholder engagement activities. In contexts where retaliation risks are prevalent, a good way to ensure that these risks get prioritized is to appoint a staff focal point for reprisals risk management and incident response. Clear protocols should also be designed, indicating who does what, how and when if incidents do occur and how any information will be shared and with whom (subject to the consent of the victims or, where they are no longer reachable, by any third parties with a reasonable mandate to represent them).

Limiting the turnover of key staff (including safeguard specialists) is also an important means to ensure a coherent response to managing risks throughout the project. By limiting staff turnover, an institutional memory of risks, agreed mitigation measures and potential responses to allegations of retaliation can be ensured. Limiting staff turnover is also important to ensure that those at risk of retaliation – or any third parties with a mandate to represent them – know to whom concerns can be communicated.

The IDB, through its ESPF, requires its Borrowers to establish a grievance mechanism to receive and facilitate resolution of concerns and grievances about the Borrower's environmental and social performance. The grievance mechanism should be scaled to the risks and adverse impacts of the project and have project-affected people as its primary user. It should seek to resolve concerns promptly, using an understandable and transparent consultative process that is culturally appropriate, readily accessible, in accessible formats, and at no cost and without retribution to the party that originated the issue or concern. The mechanism should not impede access to judicial or administrative remedies. It should consider the use of accessible formats for different physical, sensory, and/or cognitive needs. Beyond operationalising a grievance mechanism for project stakeholders, Borrowers are also expected to collaborate with the IDB's independent accountability mechanism – the independent consultation and investigation mechanism – as relevant, and, in the event of allegations of serious forms of retaliation, with competent authorities or mechanisms at national or international levels.



## Designing safe grievance mechanisms

In contexts where risks of reprisal are at issue, grievance mechanisms that have designed without considering such risks in design and operationalisation are unlikely to receive complaints, even where there may be significant concerns or grievances among project-affected communities and individuals about the Borrower's environmental and social performance. Operational-level grievance mechanisms should therefore be designed and implemented in a manner that permits stakeholders to share any concerns they have freely and without being subject to retribution from others.

In particular, stakeholders at risk of reprisal (as identified as part of the stakeholder mapping, see also Part II of the present note) should be consulted in the design of the grievance mechanism and its roll-out, including with regards engaging other authorities or actors, such as the IDB and/or its independent accountability mechanism, where stakeholders so deem necessary.

A list of questions<sup>36</sup> is provided for below to support Borrowers to design and implement safe mechanisms, and for the IDB to evaluate the robustness, from a reprisal- risk point of view, of such mechanisms.

- Have stakeholders participated in the design of the mechanism, in particular stakeholders that typically have less possibilities to expressing concerns, such as women, due to their marginalized position in society and associated concerns to their safety should they submit complaints?
- Has the mechanism been designed in a way that ensures that stakeholders feel comfortable to share information about potential retaliation they may be facing for submitting complaints, or for having done so? For example, are there multiple ways for people to submit their concerns, directly or indirectly, to the mechanism or to others, including competent authorities, IDB and/or its independent accountability mechanism?
- Have stakeholders been informed of the possibility to submit complaints to the IDB's independent consultation and investigation mechanism, and have they been informed of the mechanism's retaliation risk management guidelines?
- In contexts where there are significant concerns over security, have specific measures been taken to design and implement the mechanism in a way that does not expose complainants to risks of reprisal? For example:
  - Does the mechanism have a policy of zero-tolerance to retaliation against complainants, and has there been consistent messaging to project stakeholders, including potential complainants, that that any retribution for submitting complaints will not be tolerated?
  - How does the mechanism safeguard personal data – including the identity of the complainant(s) and any identifiable information – that has been collected in relation to a complaint and in any public

---

<sup>36</sup> The list has been adapted from [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#). IDB Invest/International Finance Corporation (2021).



reporting on handled grievances? Are complainants informed of how their data will be handled and the options for filing complaints confidentially or anonymously?

- Is there an option for complainants to submit complaints through third parties – such as local community organisations, independent lawyers, trade unionists, religious leaders, or civil society organisations – and to submit anonymous grievances? In particular, have risks of retaliation against female complainants or complainants from the LGBTQI community been adequately considered, for example, by ensuring that travelling far from communities is not necessary to submit complaints, or ensuring that there are female complaints intake and evaluation officers that are known and trusted by the women in the project-impacted communities?
- Have stakeholders been informed how concerns over retaliation can be submitted to the grievance mechanisms, and the kinds of actions that can be taken to address such concerns?
- Are there multiple entry-points for sharing information, including through, for example, a hotline, tip boxes within the project area and project area of influence, through trade union representatives (or health and safety committees where unions are not present)?
- Are proactive means to collect grievances planned, by, for example, by organising regular meetings with civil society organisations or trade unions where concerns can be raised?
- Are there any processes to notify IDB of any complaints implying significant risks of retaliation?

Where there are indicators suggesting that grievance mechanisms do not enjoy the trust of stakeholders (for example, no grievances are filed in projects associated with significant risks and impacts), it could be worthwhile to identify other actors that could be brought in to support the design and/or roll-out of the mechanism, for example national human rights institutions, human rights mechanisms or civil society organisations that stakeholders trust, or that could act as an intermediary to communicate any concerns. It should be noted, however, that such third-party actors may not always trust the legitimacy of the project in question, or the actors involved at different levels, and may for such reasons not be willing to assist.

## IDB's internal grievance protocol

With the entry into effect of the ESPF, the IDB has activated an internal protocol to address potential grievances from project stakeholders as an institutional venue to receive complaints. In this regard, the ESPF highlights that “stakeholders may submit complaints regarding a Bank-financed project to (1) the project grievance mechanism; (2) appropriate local grievance mechanisms; or (3) directly to the IDB, which will respond within a reasonable timeframe. In addition, the IDB's Independent Consultation and Investigation Mechanism provides a mechanism and process to address allegations of harm by projects as a result of noncompliance by the IDB with one or more of its operational policies, including the ESPF.”<sup>37</sup>

The IDB, through its internal grievance protocol, has an important role to play in regard to potential risks of retaliation that have been communicated to it by individuals or groups at risk of retaliation, or that allege they have been subject to acts in reprisal. Actions to address these types of disclosures will be aligned with this technical Note, including in relation to risk identification, prevention and/or mitigation efforts and responses to information that reprisals are imminent or have already occurred.

## Engaging with IDB's Independent Investigation and Consultation Mechanism (MICI)

In 2019, the independent accountability mechanism of the IDB Group, the independent consultation and investigation mechanism (MICI),<sup>38</sup> adopted [guidelines on how to assess and respond to risks of retaliation](#) as part of its complaints handling. These guidelines are intended to facilitate the effective application of MICI policies in cases where requesters, their relatives, associates or case management support staff express concern to their safety for engaging with the mechanism, or where there is pre-existing risk that may be aggravated for the fact that they chose to do so. The guidelines also apply to risks of retaliation that may be faced by local facilitators such as interpreters, translators, drivers or local “fixers” that ensure the smooth running of MICI processes, including in relation to field visits. These facilitators may face particular risks since they are sometimes perceived as “collaborating” with a “foreign agency” or otherwise seen as “delaying” or even “derailing” projects funded by the Bank.

BOX: As has become evident in dispute resolution processes of independent accountability mechanisms, local facilitators also run the risk of being subject to reprisals as they may be perceived to be directly associated with, and facilitating, investigations into sensitive matters. At the same time, local facilitators – such as drivers, translators, interpreters and “fixers” that ensure the

<sup>37</sup> Inter-American Development Bank, 2020. Environmental and Social Policy Framework, Part 1, Section 7.3.

<sup>38</sup> The MICI can receive complaints filed by two or more persons residing in the country where an [IDB](#), [MIF](#), or [IDB Invest](#)-Financed Operation is implemented, and who believe that they are being harmed or may be harmed in the future, by such operation. These persons are called Requesters or complainants. The MICI has no mandate to address complaints from IDB staff, clients, directors or other parties.

success of on the ground visits in general – may be indispensable for mechanisms to access local communities and individuals that have submitted the requests in the first place.<sup>39</sup>

Considering the safety of local facilitators is part of the IDB Group’s due diligence responsibilities, and also the due diligence responsibilities of Borrowers and implementing agencies. Where local facilitators are brought in to support project implementation, in particular in relation to sensitive processes such as those related to the MICI or Bank-led consultations with at risk individuals or groups, particular care must be taken to ensure the safety of local contractors, prior to, during and after their work.

In high-risk circumstances, ensuring the safety of local facilitators can include, for example:

- Rotating local facilitators so that the same individual or individuals are not perceived to be synonym with a specific investigation or process.
- Discussing security issues with local facilitators prior to contracting, in particular any past human rights advocacy activities that may expose the person to risk of reprisals, and agreeing on measures that could be taken – and by whom – if risks materialize.
- For online consultations requiring an interpreter, not disclosing the name of the interpreter (by noting their name during the call or asking that they sign into the meeting with their name) and not asking them to show their faces during the call.
- As feasible, keeping the identities of local facilitators confidential from potential sources of risk, including, for example, state authorities, and not disclosing any pictures as part of reporting.
- In the case of interpreters, contracting translators that speak the local language needed to do the job but that legally reside in other countries.

Amongst other, the MICI guidelines establish that in the event of imminent risk to the physical safety of requesters and in cases of arbitrary detention, MICI will determine the measures to be taken, and establish a protocol with the relevant organizations in order to access them if, and when, required. In line with the principle of participatory approach, throughout the entire process, the complainants’ views, preferences and context knowledge serve as the main input to the Risk of Reprisals Assessment and the Joint Plan to Reduce Risks of Reprisals that are foreseen by the Policy. Any decisions or actions taken by the MICI will always be determined by the complainants’ fears, views and priorities.

The MICI Director will also determine whether it’s appropriate to elevate the matter to the Board of Executive Directors and determine the usefulness and pertinence of requesting a meeting with the Board Member from the case’s country of origin, in order to jointly analyse and report on the situation. The Guidelines note that where the situation so merits, meetings may also be held with IDBG Senior Management,

---

<sup>39</sup> For a good overview of some of the particular risks that local facilitators may face, and examples of World Bank management responses to such risks and incidents involving retaliation, see World Bank Group Inspection Panel, December 2021: Emerging Lessons Series No. 7. The Right to Be Heard – intimidation and reprisals in World Bank Inspection Panel Complaints.

the country representative, and/or the project team, in order to inform and jointly analyse the situation. Effective as of 2019, the policy has been put to practical use in a number of cases, including through the conduct of dedicated risk and threat assessments for complaints handling and design of specific mitigation measures, such as ensuring confidentiality of identities of requesters.

It is worthy to note that while MICI typically requires that requesters (complainants) provide information about any previous engagement they have had, or sought to have, with IDB management over a project's environmental and social performance, this requirement is waived where requesters indicate that they fear reprisal due to engaging with Borrowers.

In general, where MICI receives requests from project stakeholders, IDB staff and clients should inform the MICI of any retaliation risks that have been identified, any incidents that may have happened, and whether specific responses have been agreed to be taken or have already been taken to address such incidents. MICI reports may also disclose any security concerns or incidents that substantiate risk of reprisal, subject to the consent of those concerned.

## 4. Address and respond to allegations of retaliation

This section outlines the steps that can be taken to respond to allegations of reprisals. It suggests that all allegations be responded to, and that the gravity of the issues raised should determine the speed at which a response is taken, with allegations implying serious concerns, such as incarceration or imminent physical danger, meriting an immediate response. Whatever response is taken, it should always be done in close consultation with, and with the informed consent of, those at risk. By default, the identity of victims should not be disclosed unless they have not given their express consent for this information to be shared as doing so risks exposing them to further risk of reprisal. The section provides useful guidance to both Borrowers, executing agencies and IDB staff, all of whom may be at the receiving end of allegations of reprisals and will need to respond to such allegations.

*Figure 3. Checklist for responding to allegations of reprisal*

- ✓ Receipt of allegation of reprisal: take all allegations seriously, even if you do not agree with them.
- ✓ Confirm receipt to the victim/source of information and inform victim/source of information about what will happen with this information, agree on how the information can be shared and with whom.
- ✓ Keep a paper trail of information and responses, limiting access to the file to a limited number of people (subject to the consent of victims).
- ✓ Where the risk of reprisal has been foreseen prior to the incident (as part of risk identification and evaluation) and a response has already been agreed, implement the response within the agreed timeline.
- ✓ If no response to the incident has been foreseen and agreed, consult the victim(s) or, if no direct engagement is possible, any third parties with a mandate to represent him/her/them and agree on the most appropriate response.
- ✓ If allegations imply serious forms of reprisal such as incarceration, the initiation of legal proceedings or imminent physical violence, act immediately, alone or in collaboration with other actors than can help.
- ✓ Maintain open lines of communication with the victim(s) and/or third parties with a mandate to represent him/her/them.
- ✓ As relevant, support the person to seek remedy for harms.
- ✓ Consider the case active and open until the person who has suffered reprisal is considered safe (in his/her/their own views).

Through its ESPF, IDB has committed to take seriously any credible allegations of reprisals. To maximise and properly manage allegations of retaliation against project stakeholders, adopting a policy of 'in doubt, report' is important for PAPs to

be able to bring forward any issues of concern to them.<sup>40</sup> A direct corollary of this approach is to take any reports of alleged retaliation seriously – even when or if the outcome is no action. Experience shows that victims of reprisal are often those who are in open opposition to projects funded by IDB and implemented by its Borrowers, may have had their credibility questioned and, in consequence, may have been entirely or partly excluded from consultative processes required by the ESPF. Therefore, where individuals or communities share concerns over potential reprisals, follow-up should not hinge solely on the perceived credibility of such stakeholders and allegations.

Standard practice from the field of protection against reprisal suggest that offering proof that reprisals have happened is the onus of those accused rather than those who claim retaliation has happened.<sup>41</sup> In other words, in the event a party faces an accusation of acting in reprisal, the burden of proof is reversed to that party. This is in recognition of the fact that those who act in reprisal, such as employers, are often able to conceal retaliatory action as justified, making it challenging for victims to access evidence to prove otherwise. A reversed burden of proof approach also recognizes that victims of reprisal may often be marginalized or excluded in general, and that power imbalances between victims and perpetrators – whether State-or non-State – should be taken into account when responding to allegations of reprisal.

In line with this approach, when raising concerns about reprisals, those who alleged that acts have been take in reprisal against them are typically required to provide the facts – what happened, when and where – and allude to the intent, that is, that the party took acts in reprisal because, for example, the alleged victim of reprisal had organized protests at the site of the project or filed a complaint with the IDB's independent accountability mechanism or publicly stated that he or she would do so. Proving that this is not the case then rests with the accused. In allegations of employment-related reprisal claims by trade unionists, for example, this can imply proving that the employment contract has been terminated due to poor work performance that predates any trade union activities, and that there are records of such poor work performance – such as annual evaluations – that attest to this.

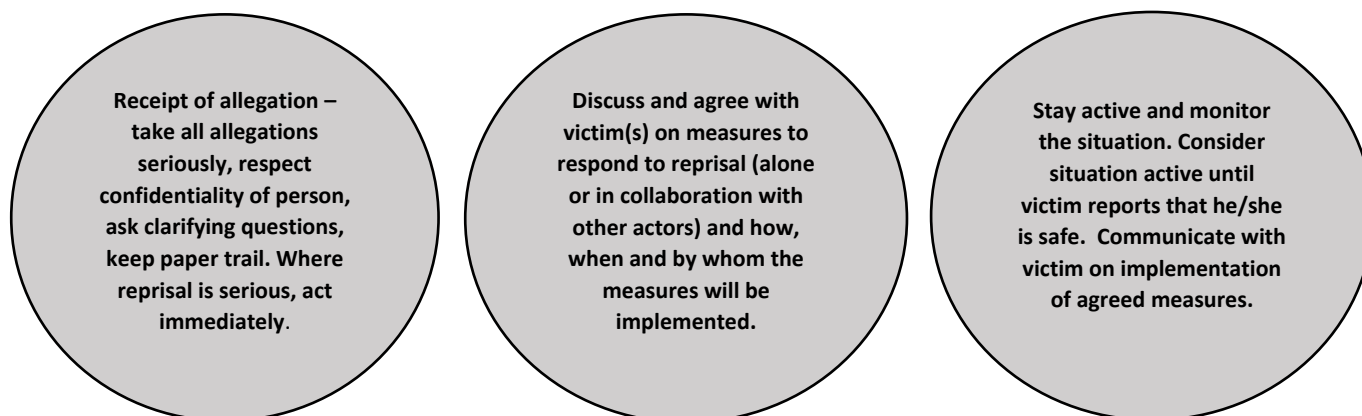
---

<sup>40</sup> [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#). IDB Invest/International Finance Corporation (2021).

<sup>41</sup> For example, the EU's Whistle-blower protection directive (adopted 2019, enters into force in 2021) reverses the burden of proof for reprisals. Recital 93 confirms that *"...the burden of proof should shift to the person who took the detrimental action, who should then be required to demonstrate that the action taken was not linked in any way to the reporting."* Article 21 (5) also requires that any detrimental measures taken must be shown to be based on *"...duly justified grounds."*

This technical note suggests three key steps to respond to allegations of reprisals:

1. Receive and review information about alleged reprisal.
2. Devise and implement appropriate courses of action, alone or in collaboration with others, and subject to consultation with the victim and his/her informed consent.
3. Stay engaged and monitor the situation until the person(s) subject to reprisals indicate that they are safe.



Depending on the alleged source of reprisal (for example actors with a role in implementing specific project activities), an independent third-party without no vested interest in the project and with the necessary expertise to safely engage with victims may be required to follow-up on the allegations.

### **1. Receiving and treating information concerning allegations of reprisals.**

Where allegations of reprisals are reported (to the Borrower or the Executing Agency or IDB, or to all three), receipt of this information should be communicated to the submitters without delay. In general, the severity of the forms of reprisal – such as arbitrary detention or the imminence of physical violence and attacks – will determine how fast information should be confirmed and acted upon, with a general rule being that serious reprisals should be acted upon immediately. At all events, acknowledging receipt of the information ensures that the person concerned knows that information has gone through and will be reviewed. It also creates an important paper trail for follow-up. Where information has been submitted not by the victim(s) but by others with a mandate to represent him/her/them or information about potential reprisals has surfaced by other means<sup>42</sup>, attempts to contact the victim(s) should be made. Prior to doing so, to the extent possible, the types of communication channels that will be used to establish contact (online – and if so, what type – or offline, and if so, where?) should be agreed upon. At times, however, it may be impossible to contact the individual or groups concerned for security or other reasons. Where security concerns are not an issue, seeking, in the first instance, to establish contact with the person/group directly impacted, without intermediaries, is important to understand their situation, what happened and what they want to happen to resolve the issue.

---

<sup>42</sup> For example, in the context of reporting by media or civil society organisations.

Once receipt of the concerns has been confirmed, as much information as possible about the alleged act of retaliation should be sought and clarified from the person(s) concerned or, where this is not possible, from other third parties with a mandate to contact him/her/them. This typically implies asking questions about what happened and when, how threats were made (directly or indirectly), whether other person(s) in the area have also been subject to reprisals, who the source of the reprisal was (if known), and what the victim(s) wish in terms of response and remedy.

Managing expectations is an important part of the contact with those at risk that are seeking protection from reprisals or remedy for reprisals that have occurred. A frank discussion should take place about what can be done, how and with whom, this is all the more important as there may be situations in which the IDB, Borrower or Executing Agency may have limited scope to engage with actors over whom they have little or no leverage. In direct corollary to this, and aligned with the ESPF, proactive building and exercising of all available forms of leverage, alone and in association with other actors who might influence the situation, is encouraged and should be informed by discussions with victims – potential or actual – of reprisals about over whom leverage should be built and how it could best be exercised.

**Box 4. The rule of thumb: do not share identity/identities of victims**

Often, ensuring the confidentiality of the identity of the victim(s) will be necessary when communicating with others, such as the source of the alleged reprisal or with other actors that could provide assistance to address the situation.

While it may be tempting to immediately contact project partners (Borrowers of executing agencies, for example) when information about reprisals has been received as a way to quickly resolve the issue, sharing the name(s) or any other personal information that could lead to the identification of the victim(s) can expose them to harm as it makes it easy to trace back allegations to an individual or group once it becomes known that such an allegation has been made and renders them vulnerable to additional reprisals for having made such a disclosure. This, in turn, undermines the possibility of ensuring confidentiality later down the line.

As a general rule, therefore, the names and any other personal information of the victim(s) of reprisal should not be shared. Put simply: the confidentiality of identities is therefore the rule of thumb and information should never be shared without the informed consent of those concerned.

Clarifying the type of information that can be shared (all, including names, or only some elements) and with whom (IDB staff/decision-makers and if so, with which staff/decision-makers, the source of the threat, national authorities, other third parties that could support responses etc.) is therefore key. A request for full confidentiality of identities requires an assessment of to what extent such confidentiality can realistically be guaranteed (for example by verifying who the victim(s) or third-party representative have already informed about the incident) and what actions should be taken if the identity or identities become



known despite measures to the contrary. Depending on circumstances, a request for full confidentiality may also hinder access to remedial outcomes, such as ensuring safe transport to and from stakeholder engagement activities. Where this is the case, those wishing to have their identities protected should be informed of the potential consequences.

## **2. Devising and implementing appropriate courses of action (what, who and when).**

Once a sufficient level of information about the event or events has been gathered a decision should be made to determine the most appropriate course, or courses, of action. This includes considering how to act, who should act and when to act.

When devising responses to allegations of reprisal, a participatory approach should be followed. This means taking into account the knowledge and views of the persons concerned when devising the measures that should be taken to respond to the situation. Measures should never be taken without the informed consent of those concerned as this can inadvertently exacerbate risks.

The most appropriate response necessarily depends on the specificities of the given situation and the wishes of victims. Depending on the situation, the support of other actors – such as human rights mechanisms or civil society organisations with specific expertise, may be needed.<sup>43</sup> In general terms, when faced with a situation of reprisal, it is important to look at what the issue is, who is the victim, and who can be mobilised and has influence over the situation.

Whether working alone or in collaboration with others, responding to allegations can imply:

- Directly engaging with the source to seek clarification on the issues raised, requesting any information on steps taken to address the situation and, in the absence of such steps, requesting that measures be taken to remedy the situation, including, as relevant, through the development and implementation of a remedial action plan, and regular reporting.
- Depending on the severity of the allegations, full collaboration with any investigations that may be underway or that may be instigated by competent authorities can also be an appropriate response. In these types of situations, requesting the intervention of authorities with jurisdiction over the source of the threat or the means to provide protective services, for example, to the victim may also be necessary.
- Supporting victims to implement their own protection and response strategies, including, as relevant, through relocation efforts.
- Supporting victims to access remedy for harms or remediating harms directly, as appropriate. Addressing reprisals may, for example, imply

---

<sup>43</sup> A list of potential sources of support organisations are included in Annex 1 to this note. This list is not exhaustive but provides an overview of the types of actors that could be approached.

remediating damage to reputation, livelihood and public standing. Victims may also need financial compensation due to reputational damage or loss of employment opportunities/income during periods of incarceration. Responses may also include public statements in support of stakeholders' right to express their views, including critical such, in a peaceful manner about the project.

- Connecting victims to support organisations at international, regional or local levels for additional support (such as, for example, rapid response actions including strengthening physical and digital security, medical assistance and psychological support).

Measures can be taken in sequence, or they can be taken in parallel.

**Box 5: The gravity of the alleged reprisal determines the speed of action**

While it is important to gather and verify information about alleged reprisals and identify measures to be taken, there may be situations where immediate action is required before claims have been verified. For example, if the person(s) concerned is in immediate danger, focus should be on reducing the source of the threat, whether through direct contact with the threat or by asking others to intervene.

The types of reprisals that, due to their gravity, requires immediate action *can*<sup>44</sup> include:

- Threats of imminent physical danger: immediate action should be taken, for example by engaging with the source of the threat directly or through others or by supporting relocation as not doing so can lead to physical harm and fatalities.
- Detention immediate action should be taken for example by engaging with local or central government as engaging will be much more challenging if the process goes from detention to actual legal charges.
- In addition, where patterns of threats have increased in severity, it is also an indication that the situation is increasingly dangerous and merits immediate responses.

If in doubt about the gravity of the alleged reprisal, any decision on immediate action should be taken based on a worst-case scenario.

As mentioned, there may be situations of reprisal in which the IDB and/or the Borrower have limited scope to engage – for example where the acts of retaliation has been committed by actors over whom IDB and the Borrower have little or no leverage, such as non-State armed groups, or where the actions that have already been taken to address the situation have not been successful. Where leverage cannot be built or exercised, identifying trusted third parties, such as international organisations, national human rights institutions, diplomatic missions, or civil society organisations with specific expertise and seeking their support for appropriate public or private diplomacy and/or engagement, may be a useful strategy where

---

<sup>44</sup> This is an illustrative list only and should not be read mechanically.

this is the case. Whatever decision is taken, communicating back to the victim(s), and ensuring his/her/their consent for any such additional measures is imperative. Ideally, such networks with key support actors should be established as part of any risk mitigation strategies so that they can easily be mobilized when need be.

**3. Staying engaged and monitoring the situation.**

As an ongoing measure, monitoring the situation and the implementation of any agreed measures should be done through regular communication with the victims or, where direct contact is not possible due to safety concerns, with other third parties with a mandate to represent him/her/them. To the extent possible, constructive engagement with the source of the reprisal should also be maintained. Lastly, where other parties – such as international organisations or civil society organisations – are supporting any measures to address the situation, communication channels with such parties should be kept open, and regular check-in done.

Typically, a situation involving reprisals should be considered ‘active’ until the person(s) that have been subject to the reprisal indicate that it is no longer the case. This implies that engagement with the situation should continue also where a project has come to an end – whether due to its agreed timespan having lapsed and the last credit having been disbursed, or because of shutdown due to security or other concerns.

**Box 6. Addressing legal proceedings**

Bringing legal charges against PAPs is increasingly used as a means of retaliation (see Box 2, SLAPPs, above). To avoid this situation, agreeing at the outset with project partners that dialogue-based means will be the method to resolve any concerns is an important means to reduce the likelihood that legal charges are brought.

If legal proceedings are already underway, expressing concerns to local or central government authorities directly, or asking other trusted third parties (such as regional / national protection mechanisms) to intervene assist to defuse the situation. Based on past experience of such engagement by DFIs, where the Bank intervenes, such interventions will typically need to come from senior-most decision-making level and likely in the form of private diplomacy. Trial monitoring with the support of expert bodies (such as the UN Human Rights Office) and public statements expressing concerns over legal charges and outcomes of legal proceedings, as relevant, can also be an important means to address the situation. As with any other measures to respond to allegations of reprisal, whatever measures are taken should be the result of discussions with the victims (or their third-party representatives) and be subject to their consent.

## **Annex I. Overview of potential support organisations for risk mitigation measures and responses to reprisals**

The list below provides an overview of organisations that could provide support for risk identification, prevention, and mitigation and, as relevant, responding to allegations of retaliation. This list does not represent an endorsement by the bank but is meant to serve as a point of reference. It should also be noted that these organisations may not always be available to provide support, and that expectations of individuals in need of their support should be managed accordingly.

Organisation	What it is and what it can do
<a href="#">Access now</a>	<p>Civil society organisation.</p> <p>Access Now’s Digital Security Helpline works with individuals and organizations around the world to keep them safe online. If at risk, Access Now can help improve digital security practices to keep out of harm’s way. If already under attack, it provides rapid-response emergency assistance.</p>
<a href="#">American Bar Association</a>	<p>Bar Association.</p> <p>Through its Justice Defenders program, the American Bar Association observes trials and other proceedings to discourage the misuse of legal processes and provides technical assistance to local counsel representing the individuals concerned. The Centre works with local partners facing threats of retaliation to develop innovative strategies to document abuses, form cross-sectoral coalitions, build public support and engage key stakeholders to increase respect for human rights in business operations. Additionally, the Centre helps activists to obtain protection when facing violent threats</p>
<a href="#">Amnesty International</a>	<p>Civil society organisation.</p> <p>Amnesty International runs a worldwide urgent action appeal to support cases of those in imminent risk of human rights violations and/or for those who have suffered human rights violations. Amnesty also runs a small relief fund for individuals who have suffered human rights violations and need financial assistance for example to be relocated for some time or for medical assistance due to the violations suffered.</p>
<a href="#">Civil Rights Defenders</a>	<p>Civil society organisation.</p> <p>Civil Rights Defenders can provide:</p> <ul style="list-style-type: none"> <li>· Digital and physical security consultations</li> <li>· Security trainings (digital, physical, psychological, etc.), but availability varies depending on budget and</li> <li>· Emergency Fund, which can fund relocation efforts, legal aid, or other costs</li> </ul> <p>necessary for the personal security of human rights defenders.</p>
<a href="#">European Union</a>	<p>Inter-Governmental organisation.</p> <p>The European Union (EU), through its guidelines on human rights defenders is an important entry point to engage with <a href="#">EU diplomatic missions</a>. The guidelines establish practical measures that EU member</p>

	<p>states can take to respond to retaliation through their diplomatic missions. These include, but are not limited to, public condemnation of threats and of attacks, urgent local action by EU missions to support individuals at immediate risk, the issuing of emergency visas and the provision of emergency shelter in EU member states.</p>
<p><a href="#">Freedom House</a></p>	<p>Civil Society Organisation.</p> <p>Freedom House's Global Fund can provide emergency funds to human rights defenders including journalists, who are under threat, attack, detention, prosecution, or otherwise at risk due to their work. Support includes financial assistance to improve their physical security, including for temporary relocation and other security related expenses, and grants for medical expenses (including psycho-social care), legal representation, prison visits, trial monitoring, humanitarian assistance, equipment replacement and dependent support if family is at imminent risk.</p>
<p><a href="#">Front Line Defenders</a></p>	<p>Civil society organisation.</p> <p>Front Line Defenders offers 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. Front Line also provides protection grants under a very flexible program that reflects needs (legal fees, medical support, relocation, hard security measures etc.), provides training and capacity building on security measures, provides rest and respite services, and maintains an Emergency contact (24/7) service.</p>
<p><a href="#">Inter-American Commission on Human Rights (IACHR)</a></p>	<p>Inter-governmental organisation.</p> <p>The IACHR can request that Member States of the Organisation of the Americas<sup>1</sup> take measures to protect specific individuals or groups at risk. Where an alleged retaliation has happened, the Commission can also request information from the State concerned, and issue recommendations regarding the situation that was reported. In addition, in the case of extremely grave and urgent situations, the Commission can refer the matter to the Inter-American Court on Human Rights 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. The <a href="#">Office of the Rapporteurship on human rights defenders</a> provides support in the specialized analysis of petitions presented to the Inter-American Commission regarding the situation of human rights defenders.</p>
<p><a href="#">JASS - Just Associates</a></p>	<p>Civil society organisation, covering Mesoamerica.</p>

	<p>JASS can provide advice on feminist protection to different organizations, institutions and women human rights defenders at risk and development of methodological tools and analysis on this issue. In Mesoamerica, JASS can also accompany women human rights defenders at risk, mobilize emergency resources, and provide access to shelters and a self-care home.</p>
<p><a href="#">Lifeline Embattled CSO Assistance Fund</a></p>	<p>The Lifeline Embattled CSO Assistance Fund is a consortium of seven international non-governmental organizations. Through Freedom House and Front Line Defenders, Lifeline provides small, short-term emergency grants to CSOs threatened because of their human rights work. Lifeline grants can address security, medical expenses, legal representation, prison visits, trial monitoring, temporary relocation, equipment replacement, and other urgently needed expenses.</p>
<p><a href="#">National Human Rights Institutions</a></p>	<p>National Human Rights Institutions (NHRIs) are State-mandated bodies, typically independent of government, with a broad constitutional or legal mandate to protect human rights at the national level. A-status NHRIs typically enjoys more powers and independence than lower-ranking NHRIs, and may be well placed to support any risk mitigation/prevention measures and/or responses to reprisals that have occurred.</p> <p>In an active retaliation-situation, the NHRI in the country concerned may be able to provide support through assuming a monitoring- and reporting role, legal or other support and facilitating contact with other third parties that can intervene.</p>
<p><a href="#">Protectdefenders.eu</a></p>	<p>Grant mechanism.</p> <p>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 implemented by a consortium of 12 international and regional human rights organisations and includes a variety of rapidly disbursed grants, including temporary relocation and other emergency grants.</p>
<p><a href="#">UN Special Rapporteur on the situation of human rights defenders</a></p>	<p>UN independent expert.</p> <p>The Special Rapporteur can engage Governments or private sector clients in private or public diplomacy over threats or other forms of retaliation. At times, Governments and private sector clients may react to prevent or address retaliation against individuals following a letter or public statement from the Special Rapporteur. The Special Rapporteur, with an extensive network of contacts, can also share additional contacts in the region that could provide support to those concerned.</p>
<p><a href="#">Office of the UN High Commissioner for Human</a></p>	<p>Department of United Nations Secretariat.</p> <p>The High Commissioner for Human Rights is the principal human rights official of the United Nations. With a global mandate, the High Commissioner is serviced by an Office based in Geneva and has</p>

<a href="#">Rights (OHCHR)</a>	<p>extensive presence at the regional and country level. As a trusted third party, OHCHR, can facilitate important support through:</p> <ul style="list-style-type: none"> <li>• Providing contextual risk information.</li> <li>• Discreetly engaging with central or local authorities of individual cases</li> <li>• Mobilising the diplomatic corps or other influential actors (EU, Special Rapporteurs of the UN, Inter-American Commission, other relevant third parties)</li> <li>• Public interventions, such as visiting the person under threat, observation of their court cases, prison visits and visits to persons under house arrest (and their families when necessary)</li> <li>• Engaging specific companies: informal or formal interventions with specific companies implied in an active retaliation situation.</li> </ul> <p>Of particular interest for IDB , OHCHR - through its <a href="#">Latin America and the Caribbean programme</a> - has field presence in the following countries: Chile (regional office), Colombia, Guatemala and Mexico (country offices), Guyana and Ecuador (human rights advisors).</p>
<a href="#">Peace Brigades International (PBI)</a>	<p>Civil society organisation.</p> <p>PBI provides:</p> <ul style="list-style-type: none"> <li>• physical presence of volunteers alongside human rights defenders (protective accompaniment)</li> <li>• dialogue with government authorities and armed forces</li> <li>• advocacy and outreach work with the international community</li> <li>• building and activating emergency support networks to prevent or respond to human rights abuses</li> <li>• raising the profile nationally and internationally of the organisations it accompanies.</li> </ul> <p>PBI currently has field presence in the following IDB Invest countries of operation: Colombia, Guatemala, Honduras, Mexico.</p>
<a href="#">Protection International</a>	<p>Civil society organisation.</p> <p>Based in Brussels, Protection International provides capacity building to individuals at risk through regional and country-based protection desks. Amongst other, Protection International implements specific work to support the strengthening of non-violent self-protection capacities for individuals and civil society organisations in rural areas in Colombia and Guatemala.</p>
Public Defenders Offices at country level	<p>In many countries in the region, the provision of legal assistance to vulnerable groups can be provided by public defender's offices, often at both state and federal levels.</p> <p>Depending on the specific circumstances of a given case, public defenders offices may be well positioned to provide advice and legal assistance to victims of reprisal.</p>
Ombudsman's Offices	<p>In Latin America and the Caribbean, many countries also provide or so-called ombudsman's offices that can play an important role in protecting human rights and responding to human rights violations and associated complaints. As an independent entity from the State</p>



	and typically free of charge, the Office of the Ombudsman may often have complementary roles to the judiciary in the resolution of conflicts.
<a href="#">Urgent Action Fund for Women's Human Rights</a>	<p>Protection Fund.</p> <p>The Urgent Action Fund for Women's Human Rights is 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.</p>
Human rights defenders' protection mechanisms at national level	<p>National level human rights defender protection mechanisms.</p> <p>As has been noted in Part I of the present note, several countries in the region have adopted specific measures for the protection of human rights defenders, such as public policies and programmes. Some countries have also put in place dedicated national protection mechanisms with a mandate to grant protective measures to individuals or groups at particular risk. Such policies, programmes and special measures may have a direct bearing on IDB projects. Note however, that some of these programmes may not enjoy the trust of their intended users (human rights defenders) and may struggle with financial and human resource constraints that prevents them from effectively meeting their mandates. Therefore, great care should be taken when considering approaching these programmes for support. As with any other measures to reduce risks of retaliation or respond to allegations of reprisal, any decision should be taken only with the informed consent of those concerned.</p>

## Annex II: Illustrative overview of national laws of relevance for retaliation risk management

The following annex provides an illustrative overview of some of the international agreements that IDB's countries of investment are parties to, and the national legal frameworks that may have specific provisions of relevance for retaliation risks. It is not an exhaustive list: IDB staff and Borrowers/implementing agencies should exercise judgment in applying the options suggested, adapting these to the specificities of each project and bearing in mind that additional laws of direct relevance may apply. In addition, IDB staff and Borrowers/implementing agencies should be wary that the legal frameworks may not be seen as adequate by those at risk of reprisal in a given project: therefore, as a rule of thumb and whenever feasible, additional measures may need to be discussed and agreed upon.

### Laws associated with the freedom of association and the right to organize, with specific protections against anti-union discrimination<sup>45</sup>

The principle of freedom of association forms part of the [ILO Declaration on Fundamental Principles and Rights at Work](#) (1998) which commits Member States to respect and promote principles and rights in relation to freedom of association, whether or not they have ratified the relevant Conventions. In other words, IDB countries of operation are bound by their commitment to the ILO Declaration on Fundamental Principles and Rights at Work, and many have enacted specific protections against reprisals targeting trade unionists (anti-union discrimination), whether through Constitutional provisions or Labor Codes.

In 2022, protection against anti-union discrimination was legally required in, amongst other, Argentina, Bahamas, Belize, Bolivia, Chile, Colombia and Costa Rica, the Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Jamaica, Nicaragua, Panama, Paraguay, Peru, Trinidad and Tobago, Uruguay and Venezuela, although as has been noted, the extent to which this protection is legally enforced greatly varies accordingly to country.

### Laws or policies of direct relevance to the protection of human rights defenders, including laws establishing national protection mechanisms

Many of the potential victims of reprisals in the context of IDB's operations classify as human rights defenders and as such, may be afforded additional and specific safeguards that have been enacted at country level. Many countries in the Latin American region and the Caribbean have adopted specific policies or laws establishing national protection mechanisms that may be of direct relevance for IDB projects. For example:

**Brazil:** The Brazilian Protection Programme for HRDs was formally established in 2004 as the official Brazilian guidelines for protection in cases of threat and risk of life involving individuals, groups or social organizations that act in the defense of human rights and fundamental freedoms. As of 2018, this programme has expanded its mandate to also protect all individuals working as communicators in Brazil

---

<sup>45</sup> <https://survey.ituc-csi.org/> provides a good overview of the regulations that apply across countries.

including journalists, bloggers, broadcasters, and media-workers who encounter threats or violence in the course of their work.

**Colombia:** Colombia's National Protection Unit was established in 2011 under the Ministry of the Interior. The unit has a prevention and protection programme focusing on the rights to life, freedom, physical integrity and security of persons, groups and communities, which establishes the duty of the State to protect human rights defenders and others through individual and collective prevention and protection measures based on a differentiated and gender-sensitive approach.

**Honduras:** On 14 May 2015, the National Congress of Honduras unanimously adopted Decree 34 2015, or the Law on the Protection of Human Rights Defenders, Journalists, Social Communicators and Justice Operators. The Law created the National Protection Council for Human Rights Defenders, Journalists, Social Communicators and Justice Operators, which acts as the steering body of the protection mechanism.

**Mexico:** The Mexican Mechanism for the Protection of Human Rights Defenders and Journalists was created by law on 25 June 2012, establishing a national protection mechanism to ensure their life, integrity, freedom and safety.

**Peru:** In 2019, the Ministry of Justice and Human Rights in Peru adopted a protocol guaranteeing the protection of human rights defenders. The protocol is directly binding only on the Directorate General of Human Rights, in the Ministry of Justice and Human Rights and issues eight areas of responsibility for the Directorate General in its work to protect human rights defenders, including designing, implementing and managing a registry of cases of risk situations for defenders, and setting up an early warning mechanism for timely action by the relevant authorities to respond to attacks or threats against defenders.

### Whistle-blower protection laws

Many countries in Latin and Central America have recently enacted whistle-blower protections in an effort to implement anti-corruption regimes. State parties to the Organization of American States Inter-American Convention against Corruption (1996) are also bound to ensure the protection of public servants and private citizens who, in good faith, report acts of corruption. In some of IDB's countries of investment, retaliation against whistle-blowers that present complaints, typically in the public sector, is prohibited.<sup>46</sup> In some Latin American and Caribbean countries, retaliation amounts to a criminal felony.<sup>47</sup> Others may lack specific legislation on whistle-blower protection measures, but have laws and policies that, in part, address whistle-blower protection.<sup>48</sup> To oversee compliance with whistle-blower protection requirements, many countries in the region work through Public Defenders Offices, Ombudspersons Offices and other public entities with similar competencies.

**Peru:** Peru has a dedicated whistle-blower law which covers public employees. Law N° 30424 and its Regulations, in force since 2018 and 2019, respectively, regulate the administrative responsibility of legal entities concerning the crimes of generic active bribery, specific active bribery, transnational active bribery, influence peddling, collusion, money laundering, assets, and financing terrorism.

**Jamaica:** In Jamaica, the Protected Disclosures Act governs the disclosure of improper conduct within the workplace and further guarantees that any employee who makes a report under the reasonable belief that the disclosure they are making is in the public interest and in good faith, will not be subject to any occupational detriment.

**Argentina:** Law No. 27,304 (i.e., whistle-blowing processes and whistle-blower protection programme). Law No. 27,304 (on whistle-blower protection) allows the reduction of penalties for defendants who give information that helps in the investigation of crimes such as drug trafficking, human trafficking, corruption, bribery, etc.

**Mexico:** Mexico's General Law on Administrative Responsibilities, in effect since July 2017, provides for a limited degree of protection of whistle-blowers. The law applies to all levels of government, including state-owned enterprises.

**Brazil:** Article 15 of Federal Law 13.964, 12.24.2019 (Anticrime Law) provides a set of protections and incentives to whistleblowers reporting criminal activity and administrative misconduct. The law applies to whistleblowers reporting general public corruption and any fraud related to government procurement and contracts, government-owned companies, and government-funded programs. But it also applies, more broadly, to criminal activities and administrative misconduct harming what the law identifies as "public interest."

### **Laws protecting journalist, including in relation to non-disclosure of their sources of information**

Journalists and social commentators may report on alleged misconduct associated with IDB projects and as such, run the risk of reprisals for doing so. In addition, where journalists and social commentators are forced to disclose their sources, they may create additional risks of reprisals to such sources. A number of countries in IDB's region of investment have enacted specific protections for journalists to keep their sources confidential, whether through Constitutional provisions or specific thematic laws. For example:

**Brazil:** Article 5 of the Constitution provides that "Access to information is ensured to everyone and the confidentiality of the source shall be safeguarded, whenever necessary to the professional activity."

**Paraguay:** Article 29 of the Constitution states that "The practice of journalism, in all its forms, is free and is not subject to prior authorization. In performing their duties, journalists of mass communication media organizations will not be forced to act against the dictates of their conscience or to reveal their sources of information".

**Ecuador:** the 1998 Constitution protects the secrecy of sources for journalists and social commentators.

**El Salvador:** In 2004, the Criminal Procedure Code was amended to provide protection for journalists. Section 187-A of this Code states that i) a journalist or a person with another profession but who has acted as a journalist, cannot be compelled to act as a witness in a judicial procedure with respect to facts or information gathered in his work as journalist and ii) the same persons have the right to refuse to provide the sources of their information.

**Haiti:** Article 28-2 of the 1987 Constitution of Haiti states that "journalists may not be compelled to reveal their sources. However, it is their duty to verify the authenticity and accuracy of information. It is also their obligation to respect the ethics of their profession."

**Chile:** under Section 7 of the Law on the Freedom of Opinion, Information and the Exercise of Journalism, "directors and editors of media, journalist, students of journalism doing training, have the right to maintain the secrecy of their sources". This privilege is extended also to the records and papers in their possession.

**Mexico:** Mexico has one the strongest laws on protections in the region. The laws on protection of sources were adopted in June 2006 by the Federal government and in the Federal District. The federal law provides that every journalist is entitled to preserve the sources of their information. It is not only a right but a duty because the journalist can only provide the source with the source's consent. They can refuse to testify as witness in a trial or procedure. It also protects their archives and telephone calls.

### Legislation on the protection of witnesses in the context of legal proceedings

Where reprisals associated with IDB projects occur in relation to – including in the lead up to, during and after – legal proceedings, and depending on the nature of such proceedings, witness protection may be of direct relevance. This type of protection would typically be afforded in criminal proceedings implying crimes of serious nature, and would be granted based on a case-by-case assessment by national authorities. A number of countries in the region run witness protection programmes. For example:

**Colombia:** Two witness protection programmes, accessed via the public prosecutor's office, were established in 1997.

**Guyana:** A Witness Protection Act was passed in 2018.

## Additional reading

Asian Infrastructure Investment Bank, 2021. [Revised Environmental and Social Framework](#).

Black, N., and Gula L., 2010. How Businesses can Encourage Governments to Fulfil their Human Rights Obligations.

Roberts, Brown, Olsen, 2011. Whistling while they work: a good-practice guide for managing internal reporting of wrongdoing in public sector.

European Bank for Reconstruction and Development, 2019. Guidelines for EBRD Personnel on handling allegations of retaliation for criticism and complaints related to the EBRD.

European Investment Bank, 2020. [Guidance Note for EIB Standard on Stakeholder Engagement](#).

FINNFUND, 2019. [Human rights statement](#).

FMO, 2017. [Position statement on human rights](#).

IDB Invest / International Finance Corporation, 2021. [Good Practice Note for the Private Sector: Addressing the Risk of Retaliation against Project Stakeholders](#).

International Alert, 2005. [Conflict-Sensitive Business Practice: Guidance for Extractive Industries](#).

Inter-American Development Bank: Independent Consultation and Investigation Mechanism, 2019. [Guide for Independent Accountability Mechanisms on Measures to Address the Risk of Reprisal in Complaint Management](#).

Inter-American Development Bank: [Independent Consultation and Investigation Mechanism, 2019. Guidelines for addressing risk of reprisals in complaint management](#).

International Finance Corporation, 2017. Good Practice Handbook. [Use of Security Forces: Assessing and Managing Risks and Impacts](#).

Institute for Business and Human Rights, 2011. [From Red Flags to Green Flags - the Corporate Responsibility to Respect Human Rights in High-Risk Countries](#).

Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the International Committee of the Red Cross (ICRC), 2017. [Addressing Security and Human Rights Challenges in Complex Environments](#).

Office of the UN High Commissioner for Human Rights. Manual on Human Rights Monitoring, [Chapter 14: Protection of Victims, Witnesses and other Cooperating Persons](#).

United Nations, 2020. Guidance Note: Protection and Promotion of Civic Space.

World Bank, 2020. [Commitments against reprisals](#).

World Bank Compliance Advisor Ombudsman, 2018. [CAO Approach to Responding to Concerns of Threats and Incidents of Reprisals in CAO Operations.](#)

World Bank Inspection Panel, 2018. [Guidelines to Reduce Retaliation Risks and Respond to Retaliation During the Panel Process.](#)

World Bank Inspection Panel, 2021. [Emerging Lessons Series No. 7 – The right to be Heard: Intimidation and Reprisals in World Bank Inspection Panel Complaints.](#)