












GOOD PRACTICE NOTE FOR THE PRIVATE SECTOR:

Addressing the Risks of Retaliation Against Project Stakeholders

IDB Invest | IFC International Finance Corporation WORLD BANK GROUP

Creating Markets, Creating Opportunities

Table of Contents

INTRODUCTION 6

What is retaliation and why is it important to the private sector? 7

Why does addressing the risks of retaliation make good business sense? 11

GOOD PRACTICE SUMMARY: 10 KEY STEPS FOR THE PRIVATE SECTOR IN SCREENING, PREVENTING, AND RESPONDING TO REPRISALS AGAINST PROJECT STAKEHOLDERS 15

1. SCREENING: IDENTIFY AND ASSESS HIGH-RISK CONTEXTS 16

Good Practice 1: Make a commitment to zero tolerance 16

Good Practice 2: Identify, assess and monitor retaliation risk factors 20

2. PREVENTION: IDENTIFY AND IMPLEMENT MITIGATION MEASURES 24

Good Practice 3: Raise awareness and build staff capacity on reprisal risk 24

Good Practice 4: Communicate and engage with stakeholders on zero-tolerance commitment 27

Good Practice 5: Adopt an open, transparent, and inclusive approach with stakeholders 36

Good Practice 6: Address risks to participants during consultation processes 37

Good Practice 7: Enhance consultations with project stakeholders where reprisal risks are significant 40

Good Practice 8: Account for retaliation risks in the project grievance mechanism 41

3. RESPONSE: RECEIVE AND RESPOND EARLY TO ALLEGATIONS 43

Good Practice 9: Have protocols for incident response and proactive resolution in place 43

Good Practice 10: Protect confidentiality of complainant identity and information 51

ANNEX A. TEMPLATE FOR POSITION STATEMENT ON ZERO TOLERANCE FOR RETALIATION 53

ANNEX B. SUGGESTED LANGUAGE: REFLECTING RETALIATION RISKS IN CODES OF CONDUCT 54

ANNEX C. KEY QUESTIONS FOR STAKEHOLDERS IN HIGH RETALIATION RISK CONTEXTS 56

Additional Resources 57

TABLES AND FIGURES

Table 1. Indicative Examples of Retaliation 10

Table 2. Hypothetical Incidents of Retaliation, and Consequences for the Private Sector 13

Table 3. Contextual Factors That Can Increase Risks of Retaliation 20

Table 4. Building Staff Capacity: Potential Interplay Between Functional Teams and Retaliation Risk 25

Table 5. Potential Options for Communicating Zero-Tolerance Statements and Integrating Them into Policies and Procedures 28

Box 1. Development Finance Institutions (DFIs) and Retaliation 14

Box 2. Examples from Companies' Public Websites on Anti-Retaliation Against Stakeholders 17

Box 3. Broader Risk Factors and Project Links 23

Box 4. Risks of Retaliation in States of Emergency 39

Figure 1. Three-Step Process for Incident Response and Resolution 50

Acknowledgements

This publication was prepared under the direction of Angela Miller, Head of the Social Cluster at the Environment, Social, and Corporate Governance Division (SEG) at Inter-American Investment Corporation (IDB Invest); Felicity Kolp, Acting Lead, Stakeholder Grievance Response at the Environment and Social Policy and Risk Department at International Finance Corporation (IFC); Hannah Blyth, Associate Environmental & Social Development Specialist at IFC; and Greg Lockard, Environmental, Social & Governance Officer at IDB Invest. The document significantly benefited from extensive comments provided through an internal and external peer review process. The authors wish to thank their IFC and IDB Invest colleagues for their contributions. They would also like to extend thanks to members of the Coalition for Human Rights in Development; the Compliance Advisor Ombudsman (CAO); the Independent Consultation and Investigation Mechanism (MICI); the Office of the United Nations High Commissioner for Human Rights (OHCHR); and the International Trade Union Confederation (ITUC) for the valuable insights and feedback they provided, and the important work they continue to do on this topic.

The coauthor of this publication is Tove Holmström, an independent consultant commissioned by IDB Invest. She is currently based in Paris, and is a former staff member of the UN Human Rights Office. Her consulting work addresses business and human rights, with a particular focus on nonjudicial grievance mechanisms. She worked with the UN Special Rapporteur on the situation of Human Rights Defenders, and the Organization for Economic Co-operation and Development (OECD) before being commissioned to produce this Good Practice Note. The design was done by Manoela Tourinho D'Abreu, Arteleria.

Copyright

© International Finance Corporation 2021. All rights reserved.
2121 Pennsylvania Avenue N.W.
Washington, DC 20433 Internet: www.ifc.org

© Inter-American Investment Corporation 2021. All rights reserved.
1350 New York Avenue N.W.
Washington, DC 20577 Internet: www.idbinvest.org

This publication has been produced by IDB Invest and IFC, and the contents of this publication are the responsibility of both institutions. Copying and/or transmitting portions or all of this publication without permission may be a violation of applicable law. IDB Invest and IFC encourage dissemination of its work and will normally grant permission to reproduce portions of the work promptly, and when the reproduction is for educational and noncommercial purposes, without a fee, subject to such attributions and notices as they may reasonably require.

Methodology

As part of the research for this publication, the consultant undertook interviews with key stakeholders, including representatives of companies, investors, civil society organizations, international and regional human rights mechanisms, and independent accountability mechanisms. These conversations are reflected in the case studies, good practice tips, and company reflections. To enable candid conversations about what can be a sensitive topic, these conversations were undertaken with the understanding that they would not be attributed. Thus, no specific individuals or institutions are named.

CAO	Compliance Advisor Ombudsman
CSO	Civil Society Organization
CSR	Corporate Social Responsibility
DFI	Development Finance Institution
E&S	Environmental and Social
EBRD	European Bank for Reconstruction and Development
FINNFUND	Finnish Fund for Industrial Cooperation Ltd
FMO	Netherlands Development Finance Company
GBV	Gender Based Violence
HR	Human Resources
IACHR	Inter-American Commission on Human Rights
ICT	Information and Communications Technology
IDB Invest	Inter-American Investment Corporation
IFC	International Finance Corporation
LGBTQ	Lesbian, Gay, Bisexual, Transgender and Queer or Questioning
MICI	Independent Consultation and Investigation Mechanism
NGO	Non-Governmental Organization
OHS	Occupational Health and Safety
OHCHR	Office of the United Nations High Commissioner for Human Rights
SLAPP	Strategic Lawsuit Against Public Participation
UN	United Nations

Introduction

In many contexts around the world, shrinking civic space, crackdowns on peaceful protesters, barriers to freedom of association, and situations of fragility and conflict are creating heightened risks for communities, workers, and project stakeholders who express themselves freely. This includes their ability to raise issues about or to oppose development projects.

The private sector has an important role to play in understanding the risks faced by stakeholders who speak out, and in creating safe spaces in which they can express their concerns. Engaging local communities, workers, and other project stakeholders is vital for sustainable and inclusive private sector development. Proactive companies promote a culture of openness; clearly communicate their anti-retaliation stance with workers, contractors, government, security forces, and communities; and address allegations of reprisals promptly when they arise.

Both IDB Invest and IFC have issued positions on anti-retaliation, as outlined in IDB Invest's Environmental and Social Sustainability Policy[1] and IFC's Position Statement.[2] Neither IDB Invest nor IFC tolerates any action by its clients that amounts to retaliation against those who voice their opinion regarding the activities of IDB Invest, IFC, or their respective clients.

The private sector has a responsibility to respect human rights, independently of the state's duties to respect, protect, and fulfill human rights. This responsibility means to avoid infringing on the human rights of others and to address adverse human rights impacts business may cause or contribute to. Meeting this responsibility also means creating access to an effective grievance mechanism that can facilitate early indication and prompt remediation of various project-related grievances. Respect for human rights includes the ability of stakeholders to engage freely, voice opposition, and raise concerns with IDB Invest, IFC, and their respective clients without fear of retaliation.

Both IDB Invest and IFC take seriously any credible allegations of retaliation and, within the scope of their respective mandates, work with clients or other appropriate partners to address them. In such instances, IDB Invest and IFC raise their concerns directly with the client or relevant party, make their position against reprisals clear, and take follow-up actions as appropriate. Any such communications and actions will be in consultation with the complainant when possible, and respecting their confidentiality. IDB Invest and IFC seek to prevent reprisals through the identification of

[1] IDB-Invest Environmental and Social Sustainability Policy, December 2020. https://idbinvest.org/sites/default/files/2020-05/idb_invest_politica_de_sostenibilidad_2020_SP.pdf

[2] IFC Position Statement on Retaliation Against Civil Society and Project Stakeholders, October 2018. https://www.ifc.org/wps/wcm/connect/ade6a8c3-12a7-43c7-b34e-f73e5ad6a5c8/EN_IFC_Reprisals_Statement_201810.pdf?MOD=AJPERES

risks in their due diligence processes and engagement with their clients and partners on environmental and social (E&S) risk management for projects.

IDB Invest and IFC have developed this guidance to provide the private sector with practical advice for screening, preventing, and responding to reprisals. The client stakeholder engagement and grievance mechanisms required by our safeguard standards are the entry point for these efforts.

What is retaliation and why is it important to the private sector?

Retaliation can include any form of threat, harassment, violence, or punitive action taken against an individual, group, or organization (such as a worker, contractor, community member, activist, human rights defender,[3] or civil society organization (CSO)) who has lodged a complaint or voiced criticism or concerns about a company or a development project. The victims of retaliation can be internal to the company or project (for example, direct and contract employees, or project personnel) or they can be external (for example community members, activists, or members of a CSO). For the purpose of this Good Practice Note, the terms retaliation, retribution, and reprisal will be used interchangeably.

Reprisals against those who voice concerns or opposition to development projects have grown in visibility worldwide. Whether it is a local community activist who is subjected to anonymous threats for raising concerns about project impacts; workers who are dismissed from their jobs for attempting to form a union; or violence used by security forces against stakeholders who oppose a development project, reprisals can take many forms, and the perpetrators are not always known. The private sector has a role to play in engaging workers and communities, and creating a safe environment in which they can raise environmental and social (E&S) concerns.

Equally important, reprisals against those who oppose a project can negatively impact a project's social license to operate, and thus its successful construction and/or operation. This is the case even if the perpetrators are not directly associated with the project, for example, government officials or community members who support the project. It is therefore important for companies to assess the risk of reprisals, develop actions to reduce their likelihood, and develop a plan to respond should they occur, even if the company already has a strong internal policy against them.

[3] Human rights defenders are defined by the United Nations Office of the High Commissioner on Human Rights (OHCHR) as people who act to address any human right (or rights) on behalf of individuals or groups. Human rights defenders seek the promotion and protection of civil and political rights as well as the promotion, protection, and realization of economic, social, and cultural rights. https://www.ohchr.org/en/issues/srhrdefenders/pages/defender.aspx

This Good Practice Note provides practical guidance to companies on how to address the risks of retaliation against project stakeholders and respond to reported incidents, consistent with the safeguard standards of IDB Invest and IFC. This document maps the actions the private sector can take in three key areas:

SCREEN

Screen for and monitor risks in the project context.

PREVENT

Raise staff awareness and build capacity, clearly communicating the company's policies and position on retaliation. Adopt an open and inclusive approach to stakeholder and worker engagement, especially with those who are at higher risk, and implement a grievance mechanism that can protect confidentiality, can provide for anonymity, and is accessible through multiple channels.

RESPOND

Have clear protocols in place, including who is responsible for receiving, investigating, and responding to allegations of retaliation from project stakeholders. Monitor cases, identify any patterns that emerge, and capture lessons learned to help prevent future incidents.

Who may be most at-risk of retaliation?



Workers who express concerns about workplace practices, including through workers' organizations (for example, trade unions)



Civil society organizations and lawyers working with project-affected stakeholders



Women may face additional risks, since they can be subjected to harassment, defamation, and physical or sexual violence



Complainants to accountability mechanisms of Development Finance Instatutions (DFIs); and local service providers, such as interpreters and drivers who facilitate the work of these mechanisms



Project-affected stakeholders and communities, in particular indigenous peoples, and other vulnerable/marginalized groups

Who may be undertaking or promoting retaliation?



Company representatives and partners, such as private security forces, suppliers, contractors and subcontractors, consultants, and financial intermediary companies



Local or central government representatives, including public security forces



Third party actors, such as paramilitary groups and criminal organizations



Community members, for example where project-affected stakeholders have differing opinions over a project

Table 1. Indicative Examples of Retaliation[4]

Type of Retaliation	Example of Retaliation	Targeted at whom?	Coming from whom?
Verbal intimidation	Threatening phone calls or visits	Family members of local community leaders	Company representatives involved in the project
Damage to property	Destruction of office computers following a targeted break-in	Community-based organization	Other community members or local stakeholders in favor of the project
Restrictions on movement	Travel bans	Community activist seeking to leave or return to the country	Central government
Criminalization	Detention without charges, or charges brought to scare people into silence	Complainants to independent accountability mechanisms	Local government
Slander or stigmatization	Individuals branded as "anti-development" or "terrorists" in the press, radio, or social media campaigns, or via the filing of strategic lawsuits against public participation (SLAPPs)	Project-affected community members	Portfolio company
Physical violence	Beatings during gatherings at project site to demonstrate against the project	Community members	Staff of private security forces contracted for the project
Digital surveillance	Interception of online communication	Civil society organization working with project-impacted communities	Central government
Physical surveillance	Project proponents attending public meetings about the project to take note of who is expressing opposition to it	Community members	Local business owners
Ill-treatment	Closing of basic services to local communities	Project-affected community that has organized public protests against the client	Public or private service provider, following requests from local government

[4] This table provides indicative examples of retaliation only, acknowledging that there are many other more forms of retaliation, and that they could come from multiple sources. It should also be noted that the source and/or nature of reprisal incidents is not always clear cut; for example, physical surveillance may come from a combination of businesses, security, and community actors.

Type of retaliation	Example of retaliation	Targeted at whom?	Coming from whom?
Discrimination in relation to employment	Allocation of undesirable, "dirty" jobs to workers active in trade unions	Workers active in trade unions	Contract company representatives involved in the project
Disciplinary action and dismissal	Targeted disciplinary action and firing of workers who have reported concerns about working conditions at the site	Workers	Company representatives

Why does addressing the risks of retaliation make good business sense?

An atmosphere of fear, mistrust, and silence created by reprisals does not create a healthy environment for business to succeed and grow in. It is not conducive to building good relationships with workers, local communities, customers, investors, or the public, and it may jeopardize the company's reputation and social license to operate.

Creating a safe and open environment for workers and communities to raise E&S concerns can help a company manage risks by proactively identifying potential problems and working with affected stakeholders to address issues before they escalate. Having open and ongoing dialogue with communities and workers builds trust, can improve worker productivity, and enhance the company's social license to operate. When project stakeholders do not feel that their concerns are being heard or taken seriously, it can lead to an escalation of tensions, increased public opposition, and polarized relations within communities. Early and upstream engagement is key to both preventing reprisals and enabling sustainable business practices.

For companies with financing from a Development Finance Institution, E&S standards require meaningful stakeholder engagement and operational-level grievance mechanisms free from fear of reprisal, so that stakeholders feel safe to share concerns and seek resolution.

What can go wrong?

The most high-profile reprisal cases making international headlines recently have focused on local community members, particularly women and indigenous peoples, who have been murdered for opposing private-sector projects. Reprisal incidents can result in loss of life, infringe on basic rights and freedoms, spark community protests, disrupt business operations, reduce company credibility with shareholders, put financing at risk, and jeopardize a business's social license to operate.



Table 2. Hypothetical Incidents of Retaliation, and Consequences for the Private Sector

Type of Project	Hypothetical Example	Consequences
 Renewable energy plant	Local community members critical of hydroelectric project affecting their livelihoods are killed.	Legal charges are brought against the company, an intergovernmental organization makes public statements, and some investors suspend their involvement in the project.
 Extractives project	Companies involved in a small-scale extractive project do not take action to address harassment of local community members campaigning against the project.	The principal investor leaves the project.
 IT software	IT companies provide a municipal government with surveillance technology to monitor the movements and communications of local activists.	Consumers boycott products, and an investor commissions an independent evaluation.

Box 1. DFIs and Retaliation

In recognition of the risks of retaliation against project stakeholders, a growing number of Development Finance Institutions (DFIs) have adopted public position statements, or included zero-tolerance for retaliation in their safeguard standards.

- In 2018, the **International Finance Corporation (IFC)** issued a position statement expressing zero-tolerance for any action by an IFC client that amounts to retaliation–including threats, intimidation, harassment, or violence – against those who voice their opinion regarding the activities of IFC or its clients.

- Through its Sustainability Policy (2020), **IDB Invest** expresses zero-tolerance for retaliation against those who voice their opinion or opposition to IDB Invest-financed projects.

- The **Finnish Development Bank (FINNFUND)**, in its human rights position statement, emphasizes that it does not tolerate threats or other forms of pressure or retaliation against whistleblowers, human rights defenders, or other stakeholders.

- The human rights position statement of the **Dutch Development Bank (FMO)** affirms that FMO does not tolerate any activity by its clients that amount to the oppression of or violence toward those who voice their opinion in relation to FMO activities and the activities of its clients, and that it will take seriously credible allegations that a client has acted inappropriately, examine the veracity, and instigate further action as and where appropriate.

- **The European Bank for Reconstruction and Development (EBRD)** 2019 statement on Retaliation Against Civil Society and Project Stakeholders stresses that they do not tolerate actions by EBRD clients or other project counterparties that amount to retaliation. They emphasize that impairing or harming (or threatening to impair or harm) any party, or the property of any party, directly or indirectly, with the intent to improperly influence the actions of that party in connection with an EBRD project constitutes a Coercive Practice under their Enforcement Policy and Procedures, and can be subject to Enforcement Proceedings.

Good Practice Summary: 10 key steps for the private sector in screening, preventing, and responding to reprisals against project stakeholders

Addressing reprisal risks requires a holistic approach. This includes creating and maintaining a culture of openness at the company; communicating clear policies and procedures on anti-retaliation to workers, contractors, partners, government, security forces, and communities; assessing the risks; strengthening systems; and being ready to address allegations of reprisals against project stakeholders.

SCREEN

1. Make a commitment to zero tolerance.
2. Identify, assess, and monitor reprisal risk factors.

PREVENT

3. Raise awareness and build staff capacity on reprisal risk.
4. Communicate and engage with stakeholders on zero-tolerance commitment.
5. Adopt an open, transparent, and inclusive approach with stakeholders.
6. Address risks to participants during consultation processes.
7. Scale up consultations with project stakeholders where reprisal risks are significant.
8. Account for reprisal risks in the project grievance mechanism.

RESPOND

9. Have protocols for incident response and proactive resolution in place.
10. Protect confidentiality of complainant identity and information.

Screening: Identify and Assess High-Risk Contexts



As part of their existing E&S risk identification processes, companies can identify contexts in which reprisal risks are elevated. Where high-risk contexts are identified, additional assessments can contribute to the design of targeted measures to address risks.

GOOD PRACTICE 1 Make a commitment to zero tolerance.

A zero-tolerance statement **from senior management** can clearly communicate expectations to both staff and business partners that the input and views of all stakeholders are valued, and that any retaliatory act – including threats, intimidation, harassment, or violence – against individuals or groups who express their views or concerns will not be tolerated. Underlying this message is an effort to reinforce a culture of transparency and access to information.

While a public commitment is not in itself enough, and needs to be coupled with institutionalization and implementation of that commitment, it does send an important signal. (See **Annex A. Template for a Position Statement on Zero-Tolerance of Retaliation**.)



Box 2: Examples from Companies' Public Websites on Anti-Retaliation Against Stakeholders

ON WORKERS:

Accenture

"Accenture has zero tolerance for retaliation against anyone who speaks up in good faith. Retaliation means any kind of unfair treatment, whether subtle or overt. There are serious consequences for retaliation, up to and including dismissal... we expect Accenture Leaders to create an environment where people feel comfortable raising their concerns."[5]

Kellogg's

"Retaliation Is Strictly Prohibited. We support honest and open communication and encourage our employees to report concerns. We will not tolerate retaliation against anyone who discloses actual or suspected violations. Retaliation will result in disciplinary action up to and including termination of employment."[6]

ON CIVIL SOCIETY ADVOCATES:

Adidas

"The Adidas Group has a longstanding policy of non-interference with the activities of human rights defenders, including those who actively campaign on issues that may be linked to our business operations. We expect our business partners to follow the same policy; they should not inhibit the lawful actions of a human rights defender or restrict their freedom of expression, freedom of association, or right to peaceful assembly. We value the input and views of all stakeholders and we are willing, and open, to engage on any issue, be this related to our own operations or our supply chain."[7]

ON BUSINESS SUPPLIERS:

BP

"We have zero tolerance for retaliation, which includes threats, intimidation, exclusion, humiliation, and raising issues maliciously or in bad faith. We want to work with business partners who share our commitments to safety, ethics and compliance and we communicate clearly our expectations of suppliers and business partners, agreeing contractual obligations where appropriate."[8]

[5] Accenture, Code of Business Ethics. https://www.accenture.com/_acnmedia/pdf-63/accenture-cobe-brochure-english.pdf

[6] Kellogs, Kellogg Company's Global Code of Ethics. https://www.kelloggcompany.com/content/dam/kellogg-company/files/EN_COE_Final1.pdf

[7] Adidas. The Adidas Group and Human Rights Defenders. https://www.adidas-group.com/media/filer_public/f0/c5/f0c582a9-506d-4b12-85cf-bd4584f68574/adidas_group_and_human_rights_defenders_2016.pdf

[8] BP. Business and Human Rights Policy. https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/sustainability/group-reports/bp-human-rights-policy.pdf

ON GOVERNMENT AND CIVIC SPACE:
Business Network on Civic Freedoms and Human Rights Defenders (including Anglo American, Unilever, ABN AMRO, and Primark)
"We recognise that defenders are important partners in identifying risks or problems in our business activities, encouraging due diligence and in the provision of remedy when harm occurs. When they are under attack, so are sustainable business practices…We strongly encourage governments to protect civic freedoms everywhere. This includes ensuring that civil society and human rights defenders are free from abuse, harassment, intimidation, physical attacks or from limitations on their rights to freedom of speech, assembly, association and movement individually and collectively."[9]

Addressing retaliation against project stakeholders rarely requires a company to start from nothing – most companies already have policies, principles, codes of conduct, and guidelines that they can build on.

Tips for developing a zero-tolerance statement:

In drafting a zero-tolerance statement, companies can consider:

- **Be clear about what is meant by zero tolerance**. For example, explain that if a company investigation of the allegation finds credible information that an employee has been involved in retaliatory action, disciplinary action will be taken in accordance with its Human Resource (HR) procedures. Response actions should be based on the nature and severity of the incident and should seek to use the leverage the company has where possible to respond.

- Include or refer to the zero-tolerance statement in **the company's existing policies and codes of conduct**, and/or **adopt it as a stand-alone statement** to give it greater visibility.

[9] Business Network on Civic Freedoms and Human Rights Defenders. Supporting Civic Freedoms, Human Rights Defenders and The Rule of Law. https://media.business-humanrights.org/media/documents/files/Statement_Public_v2.pdf

- Integrate the zero-tolerance position statement into **existing community engagement strategies** and operational-level grievance mechanisms.
- **Consider who should be consulted** in developing a zero-tolerance statement, both within the company (relevant departments) and externally (for example, in consultation with workers' representatives, or civil society organizations).
- **Designate who within the company should own the position statement and who will be responsible for implementing any commitments** made, and will have overall responsibility for coordinating responses to any potential incidents. External experts or an advisory group may be useful in providing support for this response process.

EXAMPLE

ISSUE: High-risk area for attacks against local activists.

RESPONSE: Joint statement with other companies in the region.

Local environmental activists are subject to threats and public smearing after they raise concerns about sector impacts. Companies in the region issue a joint public statement in support of the activists' right to express their concerns, and encourage authorities to investigate the attacks and protect the activists from further retaliation.

GOOD PRACTICE 2 Identify, assess, and monitor reprisal risk factors.

There is no single driver for reprisals. Risks may be present in any project. A good first step is often to identify high-risk contexts by screening for **contextual factors** that make it challenging for project stakeholders to safely voice their concerns about projects. These factors should be monitored on an ongoing basis for any changes.

Table 3. Contextual Factors That Can Increase Risks of Retaliation

Contextual factors that can increase reprisal risk	Examples of information sources
1. Curbing of civil liberties and freedom of association	
• Restricted civil society activity in the country. • Limited or no protections around freedom of association (in particular independent trade unions) and collective bargaining. • Challenges to freedom of the press.	• CIVICUS Monitor 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. • ITUC's Global Rights Index and Annual Report provides an overview of the state of trade union rights by country. • ILO's Country Supervision pages include discussion of freedom of association and other international labor standards by country. • Freedom House assesses the challenges for media and online freedom in its annual "Freedom and the Media" and "Freedom on the Net" reports, and provides scores for each by country.
2. Reports of targeting of NGOs, activists, human rights defenders, or journalists	
• Restricted civil society activity in the country. • Limited or no protections around freedom of association (in particular independent trade unions) and collective bargaining.	• Global Witness, Business and Human Rights Resource Centre, Frontline Defenders and OMCT highlight high-risk countries and cases of reprisals. • Reporters Without Borders has a World Press Freedom Index that ranks 180 countries and regions according to the level of freedom available to journalists.

• Challenges to freedom of the press.	• UN Human Rights Office field presences provide regular reporting on the situation in a number of countries, and can provide additional information on the situation on the ground. Regional human rights bodies, such as the Inter-American Commission on Human Rights (IACHR), provide precautionary measures and publish information on cases from their public hearings system. • National human rights institutions can provide information on the situation in specific regions. • **Project stakeholders**, including local, national, or international civil society organizations or community-based organizations that have information about the situation in the project area. • **Local and international news agencies**. Suggested key words for searching local or international media / internet: project area + human rights defenders; project area + attacks on local activists.
3. High levels of violence and unrest	
• A history of tension between local authorities, businesses, and communities in the area. • Significant tension between, or within, project-impacted communities over the project, or over previous projects in the area, including issues such as land rights and access to and use of natural resources. • Active or latent conflict in the area. Armed groups may be present.	• Armed Conflict Location Event Data and similar event data sources report on conflict incidents, which can be filtered by subnational location (for example, local government areas where the project is located). • **Project stakeholders**, including local, national, and international civil society organizations or community-based organizations, may have information about the situation in the project area.

Where contextual factors indicate that the risks of retaliation are high, it is important to undertake a more detailed risk assessment that takes into consideration regional and local factors. The following questions can help guide further analysis:

- Are there **particular groups that may be at higher risk of retaliation** (for example, Indigenous communities, other ethnic minorities, local communities, small-scale farmers, migrant workers, women)?

- What are the common or **potential sources of retaliation**, and what role may these have in project design and/or implementation? What influence will they have over project activities? This could include mapping of local businesses, security units, local officials, community groups, or others that may have been alleged to have been involved in the reprisals.

- What are the **local power dynamics** in the project area? Are there certain stakeholders (community leaders, government officials, company personnel, security actors) that have greater influence or power that could render others more vulnerable to reprisals and/or silencing?

- Are there heightened **risks of Gender-Based Violence (GBV)**, particularly in post-conflict contexts, that may intersect with retaliation risks? For example, is there a danger that female workers may be pressured into sexual activities in return for jobs? Is there a risk that women or members of the LGBTQ community will be harassed or targeted?

- What challenges could these contextual risk factors pose for the company's ability to meet its E&S safeguard standards, such as **effective stakeholder engagement and operational-level grievance mechanisms**? For example, if certain community members or workers are at greater risk due to the broader context, proactive stakeholder engagement and efforts to create safe spaces for them to share project-related concerns can be very important. (See **Section 2. Prevention**).

Companies may seek out the views of civil society organizations (CSOs), local trade associations, workers organizations, and external experts to triangulate information. In high-risk contexts, they may consider conducting more in-depth assessments, including on-site assessments and targeted consultations with vulnerable groups (including the socioeconomically vulnerable) to better understand and respond more effectively to risks.

Box 3. Broader Risk Factors and Project Links

Projects in high-risk contexts can increase the risk of retaliation against project stakeholders. There may be early warning signs, such as inflammatory rhetoric in the media or criminalization of outspoken project critics. Early screening for these factors is of key importance in order to prevent problems, and triangulation of sources of information can help private sector to better understand the local context and the potential actors. Examples of specific things a company may want to consider during screening include:

- **Anti-terrorism laws** that may be used to target local activists, according to NGO or media reports.
- **Digital surveillance** of local activists. (Companies may be asked to provide the government with data on local activists' email exchanges and travel patterns.)
- **Public security forces** may have a history of responding to peaceful demonstrations by communities with disproportionate use of force, and casualties may not be investigated.
- **Negative perceptions of the role of trade unions and widespread anti-union attitudes**. There may be cases of workers being prevented from organizing and/or union-busting, and/or trade union leaders being harassed or intimidated.
- **Community divisions over the potential benefits and risks** associated with development projects, with participants in public project consultations facing exclusion and/or violence.

2. Prevention: Identify and Implement Mitigation Measures



GOOD PRACTICE 3 Raise awareness and build staff capacity on reprisal risk.

Building staff capacity can help facilitate an open feedback culture and support efforts to prevent reprisals. It can be useful to involve staff, including local staff, across a wide range of functions, since teams on the ground often have direct and ongoing engagement with project stakeholders. Instruction on how to prevent and/or address reprisals can be mainstreamed as part of the existing company training. Potential topics include defining retaliation; the business case for addressing retaliation risks; common contextual risk factors; types of affected stakeholders; and possible measures for addressing risks, and investigating and responding to incidents. This should be an ongoing process that seeks to institutionalize an anti-retaliation culture throughout the company at all levels.



Table 4. Building Staff Capacity: Potential Interplay Between Functional Teams and Retaliation Risk

Functional team	Why is this team relevant?
Board and Management	Sets the tone for the company culture by encouraging an open culture that encourages communities and workers to share their concerns, and reinforcing an anti-retaliatory message to both internal and external stakeholders.
Environmental and Social Management	Responsible for identification, avoidance, and mitigation for E&S risks and impacts, including risks of retaliation against project stakeholders.
Corporate Social Responsibility (CSR)	Responsible for defining and developing CSR objectives, and may also have an important role in establishing collaborative relationships with organizations that could provide support for training, and for targeted risk assessments.
Government Relations	Serves as the principal channel of communication with government, and can play a role in engaging government on issues of concern, including risks or incidents of retaliation and communicating the importance of project stakeholders being able to express their concerns freely.
Human Resources (HR)	Manages employee concerns and often acts as a focal point for worker grievances. HR can monitor potential signs of employees being placed under increased scrutiny by supervisors or coworkers ostracizing or excluding them; inconsistent or increased performance expectations; or a sudden increase in negative documentation about an employee's performance.
Communications and External Liaisons	Directs messaging to media, financiers, government agencies, and other external stakeholders, and can be mobilized to respond to risks and incidents.
Community Relations	Has direct engagement with project-affected communities and is often a first point of contact for communities at risk of or subject to retaliation. May also have a role in operational-level grievance mechanisms.

Procurement	Sets bidding criteria and contractual requirements that can reflect zero-tolerance statements, as appropriate.
Workers' Representatives (Worker Organizations)	Manages the relationship between senior management and project workers, and can communicate any concerns about retaliation. This includes playing a role in engaging frontline-level workers and helping to address issues early to avoid escalation.
Project Site Management	Site management, and their staff, are often a first point of contact for stakeholders at the project gates, and may therefore be informed about retaliation risks or incidents.
Contractors and Suppliers	Local business partners typically have direct engagement with project stakeholders and can share information about risks or incidents. (They may also be a potential source of retaliation, and for that reason, providing effective staff training can be an important preventative measure.)
Security	Often interfacing with community members and workers, security management is responsible for ensuring training, vetting, and monitoring of the conduct of personnel and setting the use of force protocols. This includes reflecting anti-retaliation policies in codes of conduct.
Designated Individual/Team: Investigating reprisal allegations	Whether it is designated individuals in HR, community relations, management, or a third-party entity, this role is critical for receiving and responding to allegations quickly and sensitively, and putting appropriate systems in place for the protection of complainant confidentiality. (See **Section 3. Response: Receive and respond early to allegations**).
Designated Individual/Team: Owns implementation of anti-retaliation commitments	One individual, or a team, should be assigned responsibility for monitoring implementation of the anti-retaliation statement made by the company.

COMPANY REFLECTION

When we looked at what we already had in place to address retaliation, we noticed that our existing policies and codes of conduct addressed our own workforce and workers of our primary suppliers and contractors, but not others, like local community members. We decided to cast the net wider and included a reference to anti-retaliation for all project stakeholders in our supplier codes of conduct and our grievance mechanism policy.



GOOD PRACTICE 4 Communicate and engage with stakeholders on zero-tolerance commitment.

Messaging a zero-tolerance position can be an important measure in deterring potential retaliators from making retaliatory acts. Communicating a company's position on anti-retaliation also makes it more likely that project stakeholders will participate in stakeholder engagement activities and raise any concerns they may have directly with the company through the existing internal channels. This feedback loop with project stakeholders is not only helpful in preventing harm, but also in strengthening the project's ability to identify and address environmental and social (E&S) issues.

Beyond messaging, integrating zero tolerance into a company's systems and procedures is critical for internalizing a culture of openness at the company; being explicit about expectations concerning anti-retaliation with workers, contractors, partners, government,

security, communities and others; and being ready to address any allegations of reprisals against project stakeholders that may occur. This includes specific measures integrated into the labor and external grievance mechanisms and compliance systems, as well as a clear procedure for investigating allegations of reprisal and ensuring confidentiality for complainants.

Table 5. Potential Options for Communicating Zero-Tolerance Statements and Integrating Them Into Policies and Procedures

Option	Target audience
Develop a stand-alone anti-retaliation statement	Can be communicated to government, contractors, and communities during the earliest stages of project design
Include anti-retaliation in an overarching statement on E&S risk management	
Include anti-retaliation in the human rights position statement or CSR policy	
Reflect the anti-retaliation position in stakeholder engagement strategies	
Include anti-retaliation in policies and guidance documents relating to the company's operational -level grievance mechanism	
Embed anti-retaliation in trainings for project workforce, for example through discussions on how to interact with local communities in a respectful manner	
Have clear policies at the HR level, in collective bargaining agreements, and in employment contracts about reasonable grounds for disciplinary action and/or dismissal, and the process for each, creating clarity and fairness in order to avoid various forms of workplace retaliation	
Raise the company's anti-retaliation position as a matter of practice in informal discussions or meetings	
Communicate the company's anti-retaliation policy through social media	

Reflect anti-retaliation policy in bidding criteria	Portfolio companies, contractors, suppliers, consultants
Include anti-retaliation in company codes of conduct	
Reflect anti-retaliation policy in contractual and/or reporting requirements	
Reflect anti-retaliation rules in protocols for security providers and potentially also in agreements (such as Memoranda of Understanding and protocols) with public security forces	Private security forces, public security forces

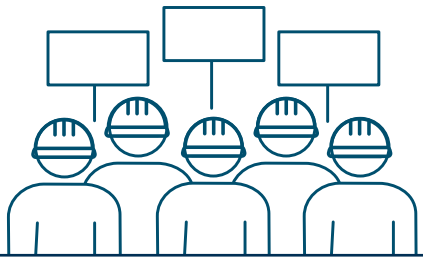
Tips for Communicating and Implementing a Zero-Tolerance Commitment

WITH BUSINESS PARTNERS

Local business partners, such as construction companies and security providers, often play a central role in project activities. These partners may be confronted with situations involving project-affected stakeholders that, if not handled properly, could result in retaliatory acts.

COMPANY REFLECTION

Some of our local contractors were not eager to let local workers join independent trade unions. There was a certain level of tension already between project workers and contractors, and harassment and blacklisting of some of the more outspoken workers had been reported. As other companies in the area had experienced similar challenges, we decided to work together to try to build a basic understanding for contractors of our expectations on trade union rights.



Tips for Engaging Business Partners

- **Commercial Requirements.** Include a brief zero-tolerance statement on retaliation in contractual arrangements or codes of conduct, with reference to the company's full statement.
- **Capacity Building.** Target training for relevant business partners on key issues such as effective stakeholder engagement and grievance management. This could be included as part of existing training or orientation materials.
- **Joint Action with Others.** Seek opportunities to adopt a common understanding with other companies operating in the same area, or together with trade unions, and communicate a collective zero-tolerance position. Establishing a joint-labor management committee for communicating and addressing issues when they arise can be another way to work collaboratively with other entities. If tensions are high between stakeholders, finding a neutral space in which to begin a process of dialogue, such as offering a "listening session" to hear opposing viewpoints, can be an effective entry point for building trust and working toward joint action.
- **Timing.** When are the best moments in the process to send messages?
  - The **early stages of engagement**, for example while defining qualification criteria for bidding processes and during contract negotiation, can be a good time to discuss issues that could arise with potential business partners.
  - During **implementation**, for example in the context of regular implementation reports; when agreeing to or renewing licenses and service agreements; when services or products require maintenance; during monitoring/audit engagements; during capacity-building activities; or along with the disbursement of funds.
  - In **response to specific events**, for example while addressing complaints from project stakeholders.

Annex B. Suggested Language: Reflecting Retaliation Risks in Codes of Conduct provides an example of a business partner code of conduct.

EXAMPLE

ISSUE: Intimidation of local communities by key project business partners.

RESPONSE: Warnings, capacity building.

Local community members participate in public consultations relating to a project. After they express concerns over impacts on cultural heritage sites in the area, they start receiving threatening phone calls from local contractors. In response, the lead company issues a notification to the contractor and requests targeted capacity-building for site staff on how to engage constructively with project-impacted communities.

WITH GOVERNMENTS

Identifying the appropriate opportunities and channels for engaging with governments concerning reprisals can be very helpful. Even when a company is not the source of a retaliation, inaction to manage retaliation risks stemming from a high-risk context can create the perception that it is associated with or condoning these actions.

Tips for Engaging Government Stakeholders

- Look for opportunities for incorporating relevant norms or expectations into **written agreements with governments**. For example, it may be possible to refer to initiatives such as the Voluntary Principles on Human Rights and Security, or to include the company's expectations in a memorandum of understanding with public security forces.
- Identify openings for engaging in **private and/or public diplomacy**. For example, companies can publicly communicate a zero-tolerance position, but engage in more detailed discussions with government actors on particular concerns.

- Identify and connect with the **appropriate government body** for addressing specific concerns. For example, if there are restrictions on public telecommunication services, companies may talk to the security branch in charge of communications, highlighting the fact that restricting mobile text messaging in times of emergency could lead to negative effects.

- Gauge interest from relevant government bodies to **build capacity** on retaliation risks. For example, public security forces can be trained in how to de-escalate high-tension situations with affected communities, and in protocols for the proportionate use of force.[10]

- Engage with **other companies** operating in the project area that may be willing to collaborate in order to address retaliation risks. They may have valuable insights or government contacts to share, and collective action may be more persuasive than each company going it alone.

- Consider opportunities for **leveraging relationships with third parties** to enhance engagement with government. It may be more effective to address some concerns indirectly by asking a third party to engage on the issues. For example, a request for support regarding certain concerns could be brought to an intergovernmental organization that has a presence in the country and relevant expertise (such as the UN Human Rights Office, diplomatic missions or other bilateral institutions).Companies might also ask their home governments to provide technical assistance to a host government in ways that could help to reduce risks. For example, one company was supported by its home government lawyers in negotiating the terms of extractive project agreements.

- Connect with **multi-stakeholder initiatives** (for example, the Extractive Industries Transparency Initiative (EITI), Voluntary Principles on Security and Human Rights (VPSHR), the Roundtable on Sustainable Palm Oil), or seek opportunities to convene a multi-stakeholder meeting to discuss how to address risks. Addressing systemic risks together with other actors can make a more convincing case and help to neutralize potential business repercussions.

[10] IFC. 2017. Good Practice Handbook. Use of Security Forces: Assessing and Managing Risks and Impacts. Guidance for the Private Sector in Emerging Markets, p. 66 for further tips on engaging government https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_securityforces

EXAMPLE

ISSUE: Violent response by public security forces toward project critics.

RESPONSE: Engagement with local police.

Members of a local community protest against a hydropower plant are beaten by public security forces guarding the project. The company seeks informal support from an international organization in the country that, without disclosing the company's request, engages directly with the provincial government and the local police to encourage them to show restraint in dealing with protestors, and urges them not to interfere when individuals are acting peacefully and within the law.

Leveraging Direct Discussions with Government

- **Consider discussing retaliation during routine meetings** rather than by organizing stand-alone meetings on sensitive issues.
- **Seek champions who may be more receptive** to efforts to manage retaliation risk. Company representatives can look for opportunities to build positive working relationships with key individuals within government who can make it easier to discuss topics based on mutual trust. Local civil society organizations and other companies in the country can help to identify the individuals within government that companies can engage with productively.
- **Set a constructive and respectful tone at the outset of the project to establish a positive trajectory for future discussions.** For example, a meeting at which issues of retaliation will be discussed should be presented as an opportunity rather than stated as a demand. It may be helpful to refer to relevant news reports or share practical and relevant case studies from the company's experience. Appealing to values such as "established good practice" can also keep the tone positive.
- **In the case of incidents of retaliation** that may be beyond the scope of the company, but that have direct impacts on its ability to do business effectively, seek opportunities to raise concerns with relevant government stakeholders or through diplomatic channels. Collaboration with other companies in a similar situation may amplify the message and encourage the establishment of an environment that supports business as well as the freedom of stakeholders to express their views.

WITH LOCAL COMMUNITIES

Clearly conveying a message of zero tolerance for retaliation against project stakeholders can signal a company's genuine commitment to this policy, and can help people feel free to express their opinions and concerns. This may include local community groups and civil society organizations (CSOs), and even local media. Companies should also consider the messenger – for example, if top management is conveying the message, it will send a powerful signal to stakeholders.

Tips for Engaging Communities

- **Identify opportunities to reinforce the company's anti-retaliatory position during meetings with project-affected communities** early in project development and on an ongoing basis. For example, the community liaison could mention it in their opening remarks at community meetings; and when company management speaks at a community event, they could reinforce the message.
- **Develop a shared understanding of the ground rules by providing examples** of what types of behavior could be considered retaliation. This can be reinforced through ongoing engagement with community members and by involving community leaders. For example, some members of the community may be concerned about the loss of economic opportunities if people express opposition to a project. Stress the idea that the company supports the ability of people to express their concerns without fear of being ostracized or harassed.
- **Emphasize the value of hearing different opinions** and the right of people to freely express any concerns they may have about the project. Provide information about how to report potential incidents of retaliation and share any company responses during community discussions or through social media.
- **Conduct stakeholder mapping** and include vulnerable members of the community in stakeholder engagement and outreach through a variety of approaches. Communicate to staff who are also community members that it is not in the company's best interest to discourage complaints.

WITH REPRESENTATIVES OF TRADE UNIONS

Issues of freedom of association, particularly in certain high-risk contexts, can result in retaliatory action against trade union officials and workers. Engaging with trade union stakeholders and reiterating a company's zero-tolerance position for reprisals to workers, union representatives, and other stakeholders, including government officials, can be helpful in reducing the risk of retaliation and general tension during negotiations.

Tips for Engaging Trade Union Representatives

- **Use collective bargaining negotiations or meetings** as an opportunity to create or strengthen procedures and policies regarding retaliation.
- **Use staff meetings with workers** to encourage the use of worker grievance mechanisms to express concerns. Stress that the company welcomes feedback, and that complaints are always kept confidential.
- **Ask sectoral or other local trade union bodies** to provide information about any history of retaliation or specific risks to consider. This can be particularly helpful for brownfield projects and projects where the company has limited knowledge of the local history of labor-related issues.

EXAMPLE

ISSUE: Criminalization of trade unionists.

RESPONSE: Engagement with appropriate authorities and joint action with other companies.

In response to the government passing a restrictive trade union law and associated criminal charges against union leaders, a group of companies in the garment industry jointly engage the government to express their concerns. They note that the credibility of their sector in the country is at stake, and request that the charges against the trade union leaders be dropped.

GOOD PRACTICE 5 Adopt an open, transparent, and inclusive approach with stakeholders.

A stakeholder engagement strategy that involves engaging with project critics can send a clear anti-retaliation message and can help a company to identify concerns and address potential issues before they escalate.

That said, company-community relationships can be challenging. When relationships with communities are strained, it may be tempting to become defensive and seek to marginalize critics. Yet if stakeholders feel that they cannot raise their concerns directly, companies are less likely to address any relevant issues before they escalate and become more difficult to resolve, potentially increasing the risks of public protests or work disruptions. Finding ways to build trust and engage with project opponents is of critical importance. If tensions increase significantly, engaging a neutral and trusted third party to help facilitate the discussion can be helpful.

Tips for Translating a Zero-Tolerance Commitment into Practical Actions

- **Maintain an ongoing dialogue with a broad range of groups** – including project opponents. Encourage coordination between community liaisons, HR, and security teams to allow workers and/or community members to protest peacefully. Seek to engage with project stakeholders even if their motivations are unclear.
- **Consider ways that the project might want to engage with local communities according to their interests and concerns, taking into account how this may** affect community dynamics, and develop engagement options accordingly. For example, it may be appropriate to hold separate meetings with various groups so that they feel comfortable speaking freely.
- **Be aware of the project benefits and employment opportunities that are being provided to communities** and avoid supporting only those community members who endorse the project. Avoid blacklisting community members, suppliers, or others who may have expressed opposition to the project.

GOOD PRACTICE 6 Address risks to participants during consultation processes.

Stakeholders may be subject to reprisals for their participation in consultations on project activities, especially if they have expressed concerns about the project. In some contexts, people may not be used to voicing or willing to voice their concerns, or there may be a strong local hierarchy in which some people don't feel comfortable speaking out in the presence of others. In such situations, consultations can be organized in such a way as to minimize the risk of retaliation and to find ways to provide safe spaces where people can share their views.

Tips for Consultations with Project Stakeholders

- **Inclusion.** Avoid meeting only with stakeholders who support the project. Organize forums where all stakeholders can be included, even those who publicly oppose a project.
- **Composition.** Consider the size and composition of consultation groups. It may be helpful to create a safe space for vulnerable and/or marginalized members of the community who may not feel comfortable speaking in large gatherings (women, indigenous peoples, members of the LGBTQ community) by conducting some sessions in smaller groups. Companies should also be aware that the presence of security personnel can sometimes be a deterrent for people to attend meetings or to speak freely.
- **Security concerns.** Consider the potential risks that participation in a consultation process may entail for some stakeholders if, for example, there are broad restrictions on the use of civic space and it is a public event. Potential safety concerns should be discussed with participants in advance, and alternative engagement options—for example private follow-up meetings—should be considered, if necessary, in order to hear everyone's perspective.

- **Facilitator.** In more challenging situations, an independent third party can be used to help build trust and facilitate dialogue with stakeholders.
- **Interlocutors.** Consider whether intermediaries, such as CSOs, trade unions, or in-country international organizations, could play a role in gauging any potential concerns related to the risk of retaliation to stakeholders or to the project.
- **Location.** Identify the best place to conduct consultations (including for focus groups or one-on-one discussions). Some locations may help to reduce the risk of surveillance. For example, meetings could be held in a neighboring village, in the capital of the country or a larger city, or in places of worship.
- **Confidentiality.** Some stakeholders may not wish to have details of the meeting recorded or sensitive discussion topics shared. Clarifying confidentiality concerns and requests with participants before commencing any consultation is key. This may include such things as deciding whether participant names will be collected and if so, how they will be stored, or whether meeting notes will be taken and if so, how they will be handled. (For example, will statements be attributed to specific individuals or groups? Will they be communicated to a select number of staff? To other project partners? Might they be made public?).
- **Electronic devices.** Where there are concerns about surveillance, it may be helpful to establish an agreement about when and where it is acceptable to store and use electronic devices (for example, recording content on phones during meetings, posting content on social media, or agreeing to leave phones off, or to remove their batteries). In high-risk surveillance settings, it may be prudent to provide a company contact point with whom participants can flag concerns or incidents.

Box 4. Risks of Retaliation in States of Emergency

Government and private-sector responses to managing natural disasters or pandemics may have implications for the risk of reprisal. For example, in the COVID-19 global pandemic and the associated government-ordered lockdowns, local activists may become targets for retaliatory measures such as arbitrary arrests and detention. In lockdowns, local activists can be easier to find, increasing the chances that they will be subject to intimidating house visits and other forms of retaliation. Suspended court hearings can also reduce legal recourse for detained individuals, and closed-door hearings can pose challenges for transparency. In some contexts, activists may even be branded as spreading the virus. Under these circumstances, enhanced monitoring of retaliation risks may be warranted. Companies may wish to consider:

- Consulting with project stakeholders who are at higher risk of reprisal regarding their preferred communication methods, and if necessary, communicating with them through secure digital channels, or third parties.
- Communicating to business partners the company's position that all stakeholder views are welcome and that retribution will not be tolerated.
- Raising concerns with governments (either individually or collectively), as appropriate.

For additional advice in the context of a global health pandemic, see IFC Tip Sheet for Preventing Reprisals During Covid-19 Pandemic.

Tips for Addressing the Risks of Retaliation in the Context of Government-Led Consultations

- **Reiterate the company's position that all views about the project – both positive and negative – are welcome.** Seek opportunities to reiterate the company's view that everyone should have the right to voice concerns about a project, or even oppose it, and not be subject to retribution for doing so.
- **Look for opportunities to express a preference for engaging a broad range of stakeholders** with diverse perspectives.
- **Reiterate that hearing from stakeholders enables the project to be designed more efficiently and responsibly,** which will help to avoid unnecessary costs and delays in implementation and can help build relationships that will make addressing future grievances.
- **Provide multiple channels for sharing views,** since some stakeholders may not feel comfortable speaking out during public consultation meetings if government representatives are there. For example, provide an online portal for (anonymous) written submissions, or via third parties.

GOOD PRACTICE 7 Scale up consultations with project stakeholders where reprisal risks are significant.

Where the risks of retaliation are significant, additional and targeted consultation can help companies understand how best to manage these risks in the project design and implementation.[11] In high-risk contexts, project-impacted communities, civil society organizations, and project workers and their representatives can often help provide a fuller picture of the risks. Religious leaders, health care providers, and teachers may be able to speak more freely about the retaliation risks faced by community members. However, it is important to recognize that influential community members can also be

[11] For more good practice on stakeholder engagement, see Stakeholder Engagement: A Good Practice Handbook for Companies Doing Business in Emerging Markets https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/sustainability-at-ifc/publications/publications_handbook_stakeholderengagement__wci__1319577185063

involved in retaliation. In complex and high-risk situations, companies can seek advice from experts, such as protection NGOs[12] and local civil society organizations, about how best to continue stakeholder engagement in these circumstances. Company representatives can also look for patterns in and escalation of incidents of retaliation, rather than looking at each case in isolation.

It is also important to recognize that company representatives may not always be best placed to engage directly with some stakeholders. Consider who may be in a better position to engage, such as a credible third party (like a local NGO) that is trusted by community members or workers.

Annex C has good questions to ask project stakeholders during consultations concerning retaliation risks.

GOOD PRACTICE 8 Account for retaliation risks in the project grievance mechanism.

An effective grievance mechanism enables stakeholders to share their concerns freely, without fear of retribution. If stakeholders do not trust or feel safe using the project-level grievance mechanism, they are more likely to seek other avenues to express their concerns or opposition.[13] It is also important to find ways to involve affected stakeholders in the design and implementation of grievance mechanisms, which will build trust and encourage more participation from workers and communities.



COMPANY REFLECTION

There were a lot of tensions over our project, but we ended up receiving almost no complaints at all through our grievance mechanism. When we asked why this was the case, we learned that most of the local communities were scared of retribution for speaking with us. We held a meeting with community leaders to discuss how we could re-design our mechanism and take such concerns into account. We also spoke with the national human rights commission to better understand the context. In the end, our complaints procedure ended up looking quite different from what we had originally planned.

[12] Some specialist NGOs and other consultancies partake in direct primary protection activities and support human rights defenders in developing their security and protection management strategies. For example, Frontline Defenders provides protection grants to at-risk human rights defenders https://www.frontlinedefenders.org/en/programme/protection-grants

[13] See Grievance Mechanism Toolkit https://www.cao-grm.org/

Tips for Adding Reprisal-Sensitive Measures in Project Grievance Mechanisms

- **Include a position statement on zero tolerance for reprisals** in the company's grievance mechanism policy.
- **Consider new or additional risks that may need to be included in the training for staff who will be handling grievances,** such as how to safely store information and ensure confidentiality.
- **Provide multiple avenues for submitting complaints** such as a hotline telephone number, online portal, tip boxes within the project area and around the community, or through trade union representatives or committees. Worker representation on occupational health and safety (OHS) committees and worker OHS representatives can help channel concerns and avoid retaliation against individuals who are raising concerns.
- **Provide an option for maintaining anonymity and the confidentiality of information** in the grievance mechanism, and communicate this clearly to stakeholders. For example, anonymous complaints could be made via an online portal, or a box placed in the staff room. Such options should supplement other avenues for lodging grievances.
- **Consider the role of third parties** such as local organizations, lawyers, trade unions that are not involved in the collective bargaining, etc., to represent complainants. For workers, having a union representative or colleague present during discussions about a grievance or during disciplinary discussions can be an effective way to reduce the fear of retaliation and intimidation.
- **Inform stakeholders** about how to communicate their fears or actual instances of retaliation. Consider communicating through multiple channels, for example, at community events, on the company website, in workplace signage, etc.
- **Seek opportunities to proactively collect grievances,** such as during regular meetings with CSOs, trade unions, community or religious leaders, and women's groups.

3. Response: Receive and Respond Early to Allegations.



GOOD PRACTICE 9 **Have protocols for incident response and proactive resolution in place.**

It is important for the company to have established protocols in place so that staff can respond promptly to reports of retaliation. This will avoid further escalation and risks to peoples' lives and livelihoods. The protocols can be integrated into the company's existing complaint response processes, for example the standard grievance mechanisms. Such a process should focus on three key areas: (1) **Receive, review, clarify**. Promptly acknowledge the complaint, gather additional information, and discuss confidentiality and possible actions with the complainant. (2) **Decide on a course of action**. Depending on what is appropriate in the circumstances, either engage directly with the source of the complaint or work with other actors to try to positively influence the situation. (3) **Monitor and report**. Report to management on any actions taken and continue to monitor events, staying in contact with the complainant and protecting confidential information, even after a resolution has been found. See **Figure 1** for details on these steps.

Tips for Responding to Incidents of Retaliation

- **Take all allegations of retaliation seriously,** not only in principle through company policies and statements, but also through timely response to and engagement with stakeholders who report incidents.
- **Have a rapid response protocol** for receiving allegations that involve imminent harm or that are time-sensitive, so that the designated person or department who is responsible can respond within a short time frame (for example, 24 hours). If incidents constitute criminal activity, such as a death threat, a company-controlled mechanism might not be the appropriate venue; in such cases, companies should consider whether engagement with the authorities is appropriate.
- **Establish a mechanism for investigating allegations** that includes provisions for how to deal with a case in which a member or members of the company are reported and are confirmed as being the source of retaliation. These should be dealt with in accordance with the company's standard HR policies related to disciplinary action.
- **Seek as much information as possible** about the incident and clarify **with whom the information can be shared.** Confirm any concerns about confidentiality considerations.
- **Act only with the consent of the complainant(s),** unless this is not feasible.[14] Acting without consent may expose the person(s) concerned to additional risks of retaliation if their identity becomes known.
- **Consider the factors that determine the most appropriate response.** This should include the nature of the alleged retaliation; the relationship with and ability to influence the source of the threat; the wishes of the complainant(s) and any security considerations; and the outcome that is sought (for example, cessation of the retaliatory acts; reinstatement of the complainant(s) to a prior condition or situation; or a public statement on project stakeholders' rights to voice concerns about the project). Where appropriate, refer the matter to competent authorities, with the consent of the person concerned.
- **Consider whether there are feasible ways to seek the support of others** who may be able to positively influence the situation. For example, other

[14] For example, if such action is required under applicable law, requiring the company to report incidents of retaliation to authorities.

companies in the region or sector, or CSOs with relevant expertise may be able to help. However, take care not to share sensitive information about the case without the person's permission.

- **Stay in contact with the complainants** when possible, and provide them with information about the actions being taken to address the situation.
- **Be aware of the need to balance transparency and the need to reduce the potential for future retaliation risks.**Choices about the level of transparency should reflect the local operating context, the relationship with the source of the threat, and the wishes of those concerned.
- **Seek constructive ways to foster learning within the company to avoid recurring incidents and to monitor risks.** By analyzing patterns of threats, the company's grievance mechanism may help to identify systemic issues and develop mitigation strategies as needed.

Figure 1: Three-Step Process for Incident Response and Resolution

Receive, Review, Clarify

Acknowledge receipt of information to show responsiveness and to document the engagement.

Gather information about the incident from the person(s) concerned or, if this is not possible, from third parties who have a mandate to represent them.

Ask the complainant what actions could best address the situation (reinstatement, public statement supporting right to peacefully protest, etc.).

Clarify with whom information can be shared. Where confidentiality is requested, assess if and how it can be maintained.

Decide on Course of Action

Directly engage with the source of the threat by:

- Communicating zero-tolerance to retaliation.
- Seeking clarification about the situation and asking for information on any steps taken to address the situation.
- Asking for full collaboration with any investigations that may be underway or that may be taken in response by competent authorities.
- Requiring that steps to address the situation be taken.
- Escalating the matter where no action / unsatisfactory action has been taken, for example by cancelling a contract.

and/or

Work with other actors to positively influence the situation. For example:

- Asking authorities to take action directly or to intervene, for example, through providing protective measures to the person(s) concerned, investigating the matter and, as appropriate, taking action against the source.
- Asking trusted third parties, such as international organisations, national human rights institutions or civil society organisation with appropriate expertise, to provide support.

As a general rule, the timing of action should be determined by the imminence and gravity of the alleged retaliation. Patterns in incidents and potential for escalation should also be considered.

Monitor and Report

Report to management and/or publicly on actions taken in a manner that does not jeopardize the safety of those concerned, for example by redacting information that might enable tracing.

Regularly communicate with the complainant(s) or, when direct contact is not possible, with third parties representing them.

Review and respond to any new information promptly.

Consider the situation "active" until the complainants indicate otherwise and continue to monitor.

Protect confidential records/information even after the incident is closed.

GOOD PRACTICE 10 Protect confidentiality of complainant identity and information.

A central principle of responding to reprisal allegations is maintaining the confidentiality of the complainant's identity and information. Seeking informed consent by explaining how the complainant's information may be used and requesting confirmation of understanding and agreement before proceeding can help contribute to the safety of the complainant and others involved in the process (for example, the company representatives handling the allegations may also be at risk).

Tips for Maintaining Confidentiality

Confidentiality protects the identity of the person as well as the information they have provided (including audio and video recordings, photographs, and/or other types of documentation) that, if revealed, could lead to their being identified and subject them to other forms of harm or stigmatization.

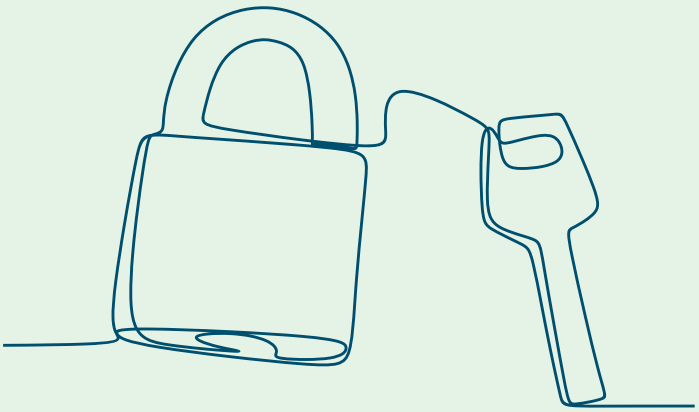
- **Inform the person about the option of requesting confidentiality.** If they request confidentiality, confirm which specific information must be kept confidential, and with whom this information can/cannot be shared (specific individuals, authorities).
- **Maintain confidentiality** through taking steps such as:
  - **Storing confidential details safely.** Physical files should be locked in a secure location and there should be limited access to electronic filing. Other technological aspects of safeguarding confidentiality may include long, varied, and regularly changed passwords; encrypted e-mails; and secured servers.
  - **Limiting the number of staff who have direct knowledge** of confidential details, or even considering third-party management of confidential information.
  - **Redacting complainant details** for wider internal communications or reporting.
  - **Having a clear strategy for maintaining confidential information** if it is transferred to other stakeholders (a different department in the company, a third party, authorities).

- **Agreeing on secure channels** to use for communication with the complainant, especially if there are concerns about eavesdropping or electronic surveillance.

- **Consider ways to gather information about the allegations without jeopardizing confidentiality** or arousing suspicion that could jeopardize the person, such as:

- **A "routine" audit of an area or activity** that covers, but is not focused solely on, the issues that have been disclosed.

- **An appropriate person "finding" relevant documentation** or evidence either by accident or in the course of their normal work.



Annex A

Template for Position Statement on Zero Tolerance for Retaliation

This template is for information purposes only and is designed for a company that wishes to adopt a zero-tolerance position statement on retaliation against project stakeholders. As with any template, the content should be reviewed and adapted for the specific situation. The draft language may also be useful for other company documents, such as Stakeholder Engagement Plans and Environmental and Social Policy statements.

COMPANY NAME
AND LOGO

We promote an open feedback culture and encourage everyone – both our own staff and external stakeholders, such as local communities and their representatives, as well as civil society organizations – to speak up in confidence, without fear of retribution, about any concerns they may have relating to our activities. We value the input and views of all stakeholders and we are willing and open to engaging on any issue related to our operations.

The nature of our operations leads us to engage with a wide range of individuals and organizations. As part of our stakeholder engagement, we seek to consult with a broad range of stakeholders, including those who are critical of issues that may be linked to our business operations. While we do not always agree with their positions, we recognize their right to express such views and we do not condone any forms of threats or intimidation, or other forms of retaliation against anyone who expresses them in a peaceful manner. We expect our business partners to condemn acts of retaliation as well.

If someone believes that they have been subject to retribution for expressing their views about our activities, they should contact us, directly or through other third parties that have a mandate to represent them, through **[insert here the relevant company function[15] that will receive and handle information relating to potential acts of retaliation]** and provide details about what has occurred. We recognize the right for this information to be submitted anonymously. If an incident is reported anonymously, sufficient information should be provided so that we can investigate the matter, as it will not be possible to directly contact the person concerned for clarification or additional detail.

In implementing this commitment, our concern will always be to safeguard the safety and well-being of any person who has brought it to our attention that they have suffered retaliation for expressing their views. We will respond to all allegations of retaliation, and to the extent possible, take action to address the situation. This may include, for example, engaging, either alone or in collaboration with others, with our business partners, government and/or other third-party actors who may be able to provide support. As retaliation may take many different forms (such as, for example, loss of a job, demotion, harassment, intimidation, violence, damage to property, and criminalization), we will respond to each incident on a case-by-case basis and seek tailored solutions.

To the extent that it does not jeopardize the personal security of those who have contacted us with concerns about retaliation, we will report, through appropriate public communication channels, the actions we have taken to address situations of alleged retaliation.

[15] Such as, for example, CSR, legal, or staff in charge of operational-level grievance mechanisms.

Annex B

Suggested Language: Reflecting Retaliation Risks in Codes of Conduct

This template is for information purposes only and is designed for a company that wishes to reflect zero tolerance for retaliation against project stakeholders in its code of conduct. It proposes language that can be included in existing codes or, depending on the level of risk, can be prepared as a stand-alone document. As with any template, the content should be reviewed and adapted to the specific situation. A clear company statement can be a powerful signal; however, it will only be effective if it is coupled with an open engagement culture embodied by the company leadership and workforce through internal and external outreach, and in its operating systems.

COMPANY NAME
AND LOGO

Business partners will create and maintain an environment that supports project stakeholders to bring forward any issues of concern to them, and where the unacceptability of acts taken in reprisal are clearly communicated to all engaged in the project.

Retaliation or reprisal is an umbrella term that refers to any detrimental action that impairs or harms, or threatens to impair or harm, a project stakeholder for having expressed opinions, concerns, or opposition over issues that may be linked to project business activities. Retaliatory acts can include, but are not limited to, any, or a combination of, the following: verbal intimidation and threat, defamation, surveillance, property damage or loss, criminalization, physical attacks discrimination, and disadvantaged or adverse treatment in relation to employment.

In order to prevent retaliatory behavior against project stakeholders, **the following core principles and minimum standards of behavior are expected to apply to all direct and subcontracted employees at all times, when at work, outside of work, and within host communities, without exception:**

a. Business partners will recognize and respect the right of project workers to join and organize associations of their own choosing and to bargain collectively. Business partners must establish and implement mechanisms for resolving disputes and employee grievances, and ensure effective communication with employees and their representatives. Workers seeking to associate freely with others, to form and join labor unions or other organizations of their choice, and to bargain collectively, or to report grievances should not be subject to discrimination, harassment, or any other form of retaliation for doing so. Engaging in, or condoning acts that amount to retaliation against workers will not be tolerated.

b. Intimidation, threats, or other forms of retaliation against external project stakeholders – including members of local communities, community-based organizations, civil society organizations or any other actors – for expressing their views, or seeking to express their views, constitute acts of gross misconduct and may be grounds for sanctions, penalties, and/or termination of employment or contract. When such acts could

constitute offenses under national law, they may, when appropriate, be brought to the attention of the relevant authorities.

c. Site managers at all levels are responsible for creating and maintaining an environment that supports open feedback and prevents acts of retaliation against project stakeholders for expressing their views. Managers will support and promote the implementation of this Code of Conduct.

d. All project workers–including contractors, subcontractors, consultants, volunteers/ unpaid workers, and interns–are encouraged to report suspected or actual acts of retaliation taken by a fellow worker, whether in the same contracting firm or not. Reports should be made in accordance with **[Standard Reporting Procedures]**.[16] Workers should feel that they are able to report such concerns without any fear of retaliation or discrimination.

e. All employees are required to attend an induction training course prior to commencing on-site work to ensure that they are familiar with this Code of Conduct.

I do hereby acknowledge that I have read the foregoing Code of Conduct, and I agree to comply with the standards contained therein; and that I understand my roles and responsibilities for preventing and responding to incidents of retaliation against project stakeholders. I understand that any action inconsistent with this Code of Conduct, or failure to take action mandated by this Code of Conduct, may result in disciplinary action.

Signed by:

_____

Title:

_____

Date:

[16] Here you can reference relevant operational guidelines or processes that the company has in place for reporting complaints.

Annex C

Key Questions for Stakeholders in High Retaliation Risk Contexts

During consultations with identified at-risk stakeholders, the following questions may be useful for better identifying risks and designing prevention measures.

Questions to ask project stakeholders during consultations on retaliation risk:

- ☐ **Have you ever been threatened or attacked** for speaking out about issues of concern to you?
- ☐ **What kinds of threats or attacks** have been made?
- ☐ **Who makes the threats?** How do you know?
- ☐ **What have they asked to be done, or told you to stop doing,** when they made these threats?
- ☐ **How would you report these threats or incidents,** if at all? Can you go to the police? If not, why not?
- ☐ **Are there times in the project cycle when the risks could be higher?** For example, when the project moves from development to construction? Around the time of local or national elections? After reports in the media have been made about project risks or impacts?
- ☐ **What kinds of measures do you think could help reduce the risks** of retaliation?
- ☐ **Do you feel comfortable with using the project grievance mechanism** to report concerns? Are there any particular issues, such as location and/or format for submitting complaints, that could help minimize the risk?
- ☐ **What are appropriate responses in the event that retaliation occurs?** Who should be contacted?

Additional Resources

Coalition for Human Rights in Development. 2019. Uncalculated Risks: Threats and Attacks Against Human Rights Defenders, and the Role of Development Financiers. https://rightsindevelopment.org/uncalculatedrisks/

IDB/MICI. 2019. Guide for Independent Accountability Mechanisms on Measures to Address the Risk of Reprisals in Complaint Management: A Practical Toolkit. http://independentaccountabilitymechanism.net/ocrp002p.nsf/0/ce43d67170fcd8f3482583a20026ab13/$file/guide_for_iams_on_measures_to_address_the_risk_of_reprisals_in_complaints_management_february_2019.pdf

IFC. 2020. Tip Sheet for IFC Clients: Addressing Increased Reprisals Risk in the Context of COVID-19. https://www.ifc.org/wps/wcm/connect/7959fcf5-3b4d-4da5-a252-42cc5544281f/Tip+Sheet_Reprisals_COVID19_June2020.pdf?MOD=AJPERES&CVID=naGtY29

International Alert. 2005. Conflict-Sensitive Business Practice: Guidance for Extractive Industries. https://www.international-alert.org/publications/conflict-sensitive-business-practice-guidance-extractive-industries-en

Investor Alliance for Human Rights, Business & Human Rights Resource Centre, and International Service for Human Rights. 2020. Safeguarding Human Rights Defenders: Practical Guidance for Investors. https://investorsforhumanrights.org/publications/safeguarding-human-rights-defenders-practical-guidance-investors

Ombudsman of New South Wales, Australia. 2017. Responding to Allegations of Reprisal Guideline. https://www.ombo.nsw.gov.au/__data/assets/pdf_file/0009/49725/Guideline-D5-Responding-to-allegations-of-reprisal-guidelines.pdf

Protection International. 2009. New Protection Manual for Human Rights Defenders. https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

Shift. 2013. Using Leverage in Business Relationships to Reduce Human Rights Risks. https://shiftproject.org/wp-content/uploads/2013/11/Shift_leverageUNGPs_2013.pdf

Disclaimer

This publication should be used only as a source of information, guidance and analysis to be applied and implemented by each user in its discretion in accordance with its own policies and applicable laws, which may or may not require all or any of the described practices to apply to its own activities and investments. This publication does not alter or amend any institution's policies and each of IDB Invest and IFC may not require all or any of the described practices in this publication in its own investments, and in its sole discretion may not agree to finance or assist companies or projects that adhere to those practices. Any such practices or proposed practices would be evaluated by IDB Invest and IFC on a case-by-case basis with due regard for the particular circumstances of the project.

In making this publication available, neither IDB Invest nor IFC is suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IDB Invest or IFC agreeing to perform any duty owed by any other person or entity to another. Professional advice of qualified and experienced persons should be sought before entering (or refraining from entering) into any specific project activity.

Neither IDB Invest nor IFC (or their respective employees or representatives) warrants or guarantees the accuracy, reliability or completeness of the content included in this publication, or the conclusions or judgments described herein, and neither accepts any responsibility or liability with respect to the use of or failure to use or reliance on any information, methods, processes, conclusions, or judgments contained herein.

The boundaries, colors, denominations, and other information shown on any map in this publication do not imply any judgment on the part of IDB Invest or IFC (or their respective employees, representatives or affiliates) concerning the legal status of any territory or the endorsement or acceptance of such boundaries. The findings, interpretations, and conclusions expressed in this publication do not necessarily reflect the views of the Executive Directors of any members of the World Bank Group, of the Board of Executive Directors of the Inter-American Investment Corporation, or the governments they represent.

Certain parts of this publication may link to external Internet sites, and other external Internet sites may link to this publication. IDB Invest and IFC are not responsible for the content of any external references.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the respective privileges and immunities of IFC or IDB Invest, all of which are specifically reserved.