Assessing and mitigating risks of reprisals for UN engagement

A TOOL FOR HUMAN RIGHTS DEFENDERS

For many human rights defenders around the globe, the United Nations (UN) is a vital platform to document and denounce abuses, allow victims to share their testimonies, and advocate for an international response to human rights crises.

The participation of human rights defenders allows the UN to make informed decisions regarding actions to take against governments or individuals perpetrating human rights violations, and to promote human rights standards globally.

The **right to safe and unhindered access to and cooperation with the UN**, and to be **free from any form of intimidation or reprisals**, is both a fundamental human right and essential to the UN's work.

Yet, when engaging, or seeking to engage with the UN, many human rights defenders and civil society organisations face acts of intimidation or reprisals. This can range from threats, online smearing, and travel bans, to disappearance or arbitrary detention, by governments, companies or others.

> ISHR has compiled all cases of reprisals documented by the UN in this database.

These acts may be aimed at **preventing their participation** or **creating fear** among others. Anyone engaging with the UN should be fully aware that, as important as it can be, doing so could increase their exposure to intimidation or reprisals. Because the UN system can seem remote, defenders sometimes underestimate the risks that arise from engaging with it.

This explainer provides tools and tactics for human rights defenders seeking to engage with the UN to **better assess and mitigate these risks**. If you are a human rights defender seeking to engage with the UN, read this carefully and share it with your peers!

> These are tools to mitigate and address reprisals for engaging with the UN specifically, but you can use them to assess risk in other circumstances of your human rights work too!

To conduct an effective **risk mitigation strategy**, you should:

- Develop a thorough **risk assessment**, ideally peer-reviewed, and constantly updated;
- Decide on the level of risk you are willing to take;
- Develop a **contingency plan** with measures intended to decrease your vulnerabilities and increase your capacities.

ASSESSING RISK

You should **always do a risk assessment before embarking on any engagement with the UN**. This allows you to think through the possible consequences that might arise according to your specific, individual context.

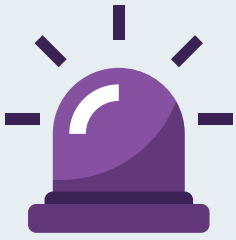
Keep in mind that your **relatives**, **colleagues**, **associates** and **organisations** may be at risk as well. Consider them as potential targets, both direct and indirect, when evaluating risk.

Firstly, what do we mean by 'risk'?

RISK = THREATS x VULNERABILITIES / CAPACITIES

Risk = the impact and probability that a threat materialises (here: for engaging or seeking to engage with the UN)

> The impact and probability of risk depend on personal and contextual factors that may or may not be under your control.



Threats = negative events that could materialise against you, your colleagues, associates or organisation

> A threat exists regardless of your actions (eg. this government often detains individuals engaging with the UN).

Vulnerabilities
= negative factors that expose you to threats or increase their likelihood or impact.

Capacities
= positive factors that reduce your exposure to threats or decrease their likelihood or impact.

Step 1: Assessing potential threats

Identify existing threats. Assess the **impact** they would have if they materialise and the **probability** this would occur by considering:

- **Type of perpetrator:** Is the threat from a State actor, non-State actor, or other entity? Does that actor have a track record of intimidating or retaliating against those cooperating with the UN (see ISHR's Reprisals Database)?
- **Victim profile:** Are the targets human rights defenders themselves, their families, or their organisations?
- **Nature of threat:** Could the threat be physical, psychological, digital, informational, reputational, political, environmental, financial, related to human resources, logistical, or of another nature?

Examples of threats include, but are not limited to:

- Threats and intimidations (online and offline)
- Surveillance (online and offline)
- Defamation, including online smearing
- Travel restrictions
- Expulsion or visa denial
- Physical attacks
- Detention and imprisonment
- Enforced disappearance, kidnapping
- Criminal investigation and prosecution
- Property damage, raid, search and asset confiscation
- Profession-related reprisal
- Targeting of relatives, colleagues or friends
- Administrative reprisal
- Access blocked to a UN expert or mechanism
- Access denied to UN premises
- Deterioration in detention conditions

Step 2: Assessing your vulnerabilities and capacities

Your existing vulnerabilities and capacities could be digital, informational, physical, organisational, legal, political, social, psychological, logistical or financial in nature. Very often, one is the opposite of the other (eg. a vulnerability might be that "I don't have access to a lawyer" vs. a capacity might be that "I have access to a lawyer").

Use the table below to map out your threats:

Impact	Probability: Low	Probability: Medium	Probability: High	Probability: Very High
Low				
Medium				
High				
Very High				

Use the table below to assess your vulnerabilities and capacities:

	Vulnerabilities	Capacities
Digital	*E.g. Unsecure devices; lack of access to Internet or telecommunication; uneven implementation of security policies; lack of IT and digital security knowledge.*	*E.g. Updated IT devices; digital security knowledge; access to trainings.*
Informational	*E.g. Possession of highly sensitive information.*	*E.g. Ways and means to protect highly sensitive information, online and offline.*
Physical	*E.g. : Medical conditions. geographical context; lack of social security and health support.*	*E.g. Being in good health; having access to adequate medical care .*
Organisational	*E.g. Lack of organisational policies; lack of legal status; unhealthy work environment; lack of contingency plans; lack of safety measures in the office (camera, lock…).*	*E.g. Safety of location; emergency contacts, including local and diplomatic; existing security plan.*
Legal	*E.g. Lack of legal knowledge; lack of access to a lawyer; irregular migration status; lack of travel documents.*	*E.g. Access to lawyers; knowledge of legal context including your rights as a citizen and international protection framework for human rights defenders.*
Political	*E.g. Sensitivity of issue; nationality; political and legal context (including restrictive laws); lack of diplomatic or other international support; lack of public visibility or, on the contrary, too much visibility.*	*E.g. Access to diplomatic or other international support; public visibility can also be a capacity insofar as it can be protective (depends on the context).*
Social	*E.g. Gender, SOGIESC (sexual orientation, gender identity, gender expression and sex characteristics), race, ethnicity, religion, economic status, or other grounds for discrimination in the society or community you live in; linguistic barriers; lack of support networks; family still inside the country if you are in exile; mistrust within family, or communities.*	*E.g. Access to a support network on the ground or online; knowledge of language; support from relatives and persons of trust.*
Psychological	*E.g. Anxiety; inability to manage stress or fear; post-traumatic stress disorder (PTSD) and other psychiatric/psychological conditions; lack of adequate psychosocial support and access to therapy; unstable emotional state; disruptive life factors (family, relations, etc); identity markers (i.e. LGBTQI+).*	*E.g. Being able to manage stress and fear; access to periodic or regular, adequate psychosocial support; well-being practices; support groups; allowing oneself to disconnect.*
Logistical	*E.g. Lack of travel insurance(flight and accommodation); visa uncertainty;*	*E.g. Support with travel arrangements.*
Financial	*E.g. Lack of sustainable source of income; lack of contingency funds; donor dependency.*	*E.g. Sufficient financial resources, including to address contingencies; knowledge of urgent grants available for human rights defenders.*

MITIGATING RISK

Once you have carried out your risk assessment, you can now plan your **risk mitigation strategy** that includes measures to **decrease your vulnerabilities**, **increase your capacities**, and a plan to **address the risks you've identified**.

Your risk mitigation strategy should at least include measures to address *all risks with high impact, and/or high probability.*

> If you have additional time and resources, consider taking all measures against other threats with medium/low likelihood and/or impact.

First, revisit your risk assessment, identify which threats you are prioritising to address, identify which vulnerabilities related to that threat you want to and can decrease, and which capacities you want to and can develop or increase.

Measures for the **prevention** of threats from occurring include:

- **Inform and plan:** Decide who you'll inform about your activities and who they should contact if something goes wrong.
- **Discuss risks:** Talk with relatives and associates about what to do and who to contact if you're unable to.
- **Protect the vulnerable:** Ensure relatives or associates at risk are in a safe place.
- **Know your rights:** Understand what to expect if you're detained or arrested.
- **Have legal support ready:** Identify a lawyer or legal contact in advance.
- **Build support networks:** Connect with international NGOs, UN mechanisms, or other organisations.
- **Use physical and online security tools:** Consider VPN options, password managers and other digital security tools, cameras and other physical equipment.

Then, develop a **contingency plan** in case, despite your best efforts to reduce risk, these threats do materialise.

> **Important:** Remember there's no 'risk-zero' approach: instead, use these tools to identify the degree of risk you are willing to take in your engagement with the UN, and tactics to mitigate those risks.

Measures to take for **protection** when threats occur include the following (consider whether private or public action will be most effective):

- **Report threats:** File complaints with local police, national authorities, if it is safe to do so, or UN security.
- **Report online threats:** Report harassment to social media companies.
- **Alert key contacts:** Keep a list of embassies, media, community leaders, NGOs, journalists, and others who can help (including through diplomatic guidelines for the protection of activists).
- **Seek local support:** Contact national human rights bodies, ombudsman offices and protection mechanisms for support.
- **Inform your network:** Inform organisations or networks of human rights you're part of, and agree on how they can assist.
- **Emergency assistance:** Gather contact details of groups that help at-risk individuals and know what they need to assist you.

Important: if you experience intimidation or reprisals for engaging with the UN, there are many UN mechanisms that can receive and address those cases, publicly and privately. Click here to learn more, and don't hesitate to reach out to ISHR for assistance.

Now it's your turn: prepare your own contingency plan!

Threats	Measures to increase capacities and reduce vulnerabilities	Contingency measures to adopt if the threat materialises

Important: We encourage you to discuss and review your risk assessment and contingency plan with trusted relatives or peers. But remember these are individualised and contextualised: each individual or organisation has a different risk profile.

Sources: Front Line Defenders, Freedom House, OHCHR, Protection International