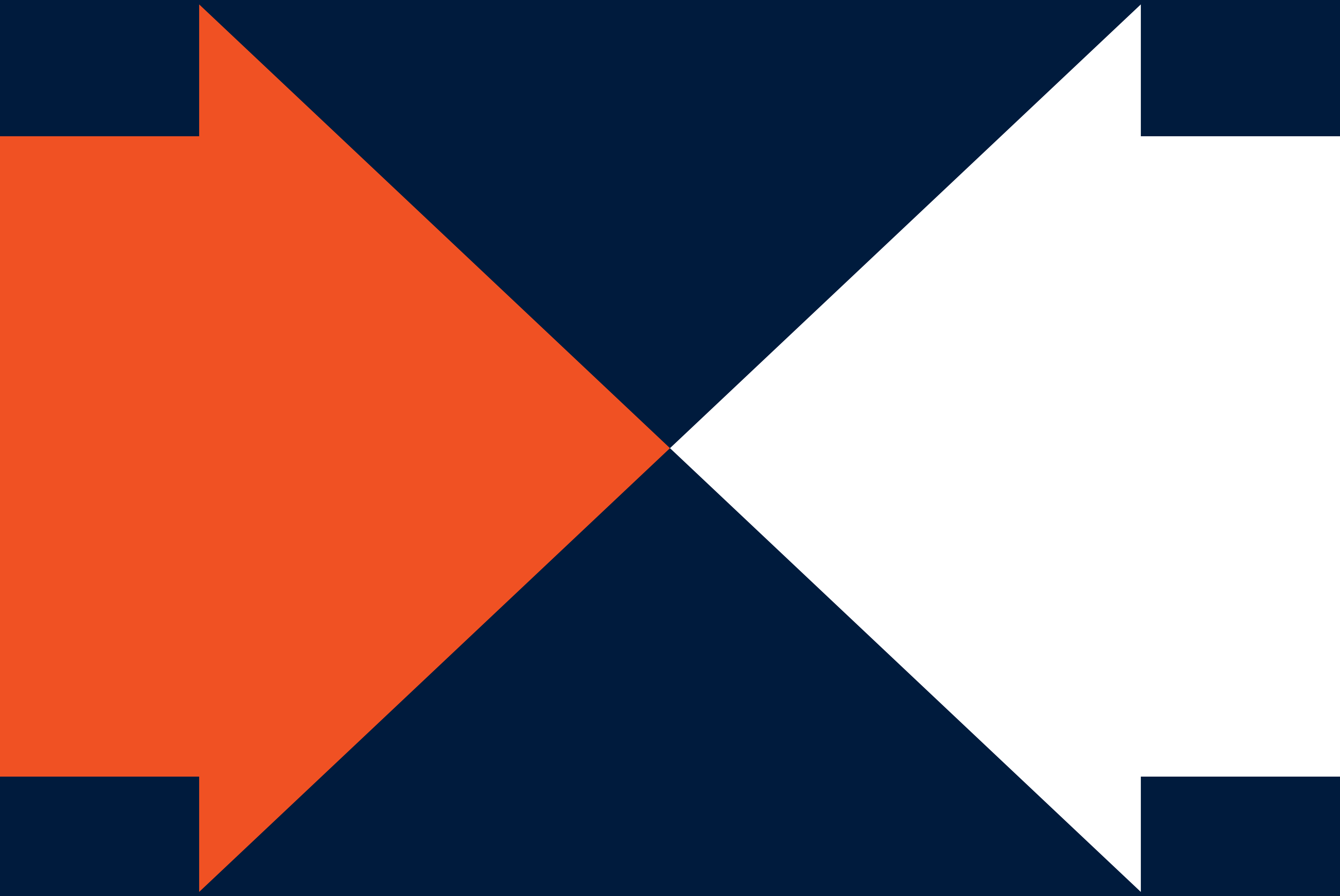


CONFLICT-SENSITIVE HUMAN RIGHTS DUE DILIGENCE FOR ICT COMPANIES

Guidelines and Toolkit for Corporate Human Rights Practitioners

BSR

JUSTPEACE
Labs

CONFLICT-SENSITIVE HUMAN RIGHTS DUE DILIGENCE FOR ICT COMPANIES

Guidelines and Toolkit for Corporate
Human Rights Practitioners

This publication was authored by Jennifer Easterday with significant contributions by Ayesha Khan and Hana Ivanhoe. Thanks to Jenny Vaughan, Lindsey Anderson, and Dunstan Allison-Hope from BSR who provided invaluable feedback. We'd also like to thank the many individuals from tech companies, academia, and civil society that we interviewed and who contributed helpful insights for this toolkit.

Special thanks to Google and Meta for providing financial support for this guidance.

Content

About This Toolkit 4

Why do tech companies need to conduct enhanced human rights due diligence? 4
What is eHRDD? 5
What is the aim of this guidance? 6

Enhanced Human Rights Due Diligence in 9 Steps 7

1 Develop a Formal eHRDD Policy and an eHRDD Process 8

1.1. Base the eHRDD process on existing HRDD processes . 8
1.2. Plan for contingencies 9

2 Build and Strengthen Cross-Functional Capacities . 10

2.1. Leverage existing teams and capabilities 10
2.2. Build eHRDD capacities across teams 10

3 Scope eHRDD Application: Triggers and Thresholds for eHRDD 11

3.1. Establish criteria for when to apply eHRDD 11
3.2. Develop a list of relevant CAHRAs 12
3.3. Define parameters for eHRDD by gathering internal data on relevant markets and business activities 12
3.4. Conduct proportionate risk tiering of CAHRAs 13
3.5. Establish and maintain a system for monitoring new CAHRAs, updating risk tiers, and escalation procedures 15

4 Conduct a Conflict Assessment 16

4.1. Understand the context. 17
4.2. Understand the interaction between activities and context 18
4.3. Assess International Humanitarian Law 19
4.4. Take steps to minimize adverse impacts and maximize positive impacts 20

5 Analyze Actual and Potential Impacts 20

5.1. Identify vulnerable groups 20
5.2. Identify conflict and human rights impacts 21
5.3. Assess salience (severity and likelihood) of impacts. . . . 23
5.4. Conduct proportionate risk tiering of impacts 25
5.5. Examine attribution 25
5.6. Assess leverage 26

6 Address Impacts 27

6.1. Integrate conflict sensitivity for mitigations 27
6.2. Ensure that mitigations are proportionate to the risk of harm 27
6.3. Track the effectiveness of mitigation measures 28
6.4. Devise a plan and strategy for when to roll back mitigations 29
6.5. Build mitigations into existing and planned cross-organizational outputs 29
6.6. Consider responsible exit 29
6.7. Provide operational level grievance mechanisms 30

7 Communicate Progress 31

8 Cross-Cutting Issue: Stakeholder Engagement 32

8.1. Build a specific eHRDD engagement strategy 32
8.2. Create context-appropriate engagement processes 33
8.3. Plan ahead 33
8.4. Garner resources 34
8.5. Take a cross-functional approach. 34
8.6. Ensure holistic, sustained, and meaningful engagement with diverse rightsholders 35
8.7. Engage with business groups, governments, and conflict actors 35
8.8. Anticipate and plan for barriers to access 36
8.9. Ensure balance and address potential bias 36
8.10. Assess and plan for security concerns 36
8.11. Be creative and flexible, and use third parties 37
8.12. Consider different ways to engage 37

9 Cross-Cutting Issue: Leverage Industry-led and Multi-stakeholder Collaboration 38

Toolbox 39

Additional reading. 39
UNGPs relevant for enhanced HRDD in CAHRA. 40
Leveraging internal teams beyond the human rights team. . . 41
External sources for CAHRA list 42
Internal data on relevant markets and business activities. . . 43
Salience measurement: sample tool 44
CAHRA risk tiering: sample tool 44
Guide to understanding the conflict 44

About This Toolkit

Why do tech companies need to conduct enhanced human rights due diligence?

The last decade has seen increases in state fragility and the number of violent conflicts around the world and a decrease in the rule of law.[1] Conflict-affected and high-risk markets are often characterized by serious human rights violations and severe harm to individuals—including loss of life, basic freedoms, or livelihoods. Companies operating in these contexts face heightened risks of being involved with those human rights harms, and risk exacerbating conflict and instability through hiring and procurement decisions, partnerships with local entities, compliance with local laws, or by the use of their products and services. This exposes companies to potential reputational damage, interruptions in business operations, legal liability, and financial penalties.[2]

The tech industry has a particularly complex nexus to conflict and instability. Emerging digital technologies have become increasingly essential and ubiquitous factor in our lives, communities, and societies. At the same time, there is increasing evidence of technology's role in exacerbating conflict. Moreover, the malicious use or disruption of technology to undermine international peace and security is a growing concern among states[3] and regulators.

Conflict, fragility, and human rights are closely linked: grievances over human rights violations can destabilize and drive conflict, while violent conflict creates additional fragility and heighted human rights risks. The UN Guiding Principles on Business and Human Rights (UNGPs) call on companies to conduct heightened—or more in-depth—due diligence in conflict settings due to the proportionately higher risk of adverse human rights impacts. See the "Toolbox" for a list of relevant Principles from the UNGPs.

*The UNGPs call for heightened due diligence in conflict settings due to the **proportionately higher risk** of adverse human rights impacts.*

[1] Palik, Júlia; Siri Aas Rustad and Fredrik Methi (2020). "Conflict Trends: A Global Overview, 1946–2019.", PRIO Paper. Oslo: PRIO. See data available at Uppsala Conflict Data Program, https://ucdp.uu.se/encyclopedia.

[2] BSR (2021). "Business in Conflict-Affected and High-Risk Contexts."

[3] UN General Assembly (2021). "Open-ended working group on developments, in the field of information and telecommunications in the context of international security, Final Substantive Report", A/AC.290/2021/CRP.2, 3.

eHRDD is, in essence, HRDD + conflict sensitivity. It requires identifying human rights impacts as well as conflict impacts.

What is eHRDD?

Heightened HRDD or eHRDD is, in essence, HRDD + conflict sensitivity. It requires identifying human rights impacts as well as conflict impacts.[4] For tech companies, conducting eHRDD in conflict-affected and high-risk areas (CAHRA)[5] poses unique challenges and requires a rethinking of how technology can impact conflict and pose heightened risks of human rights harms.

Due to the vast diversity in business models, products, services, and technologies used in the tech industry—such as social media platforms, search engines, facial recognition, AI, machine learning, cloud computing, software companies, quantum computing, telecommunications, and network infrastructure—no two due diligence processes will be the same.[6] However, there are clear phases to eHRDD and concrete steps all tech companies should take.

What are CAHRA?

CAHRA are "areas in a state of armed conflict or fragile post-conflict as well as areas witnessing weak or nonexistent governance and security, such as failed states, and widespread and systematic violations of international law, including human rights abuses."[7] They can include situations of mass violence as well as areas with weak governance or rule of law; extensive corruption or criminality; significant social, political, or economic instability; historical conflicts linked to ethnic, religious, or other identities; closure of civic space; and a record of previous violations of international human rights and humanitarian law.[8]
—Business in Conflict-Affected and High-Risk Contexts, BSR

[4] United Nations Development Programme (2022), "Heightened Human Rights Due Diligence for business in conflict-affected contexts: A Guide," notes that "Heightened human rights due diligence means identifying potential and actual impacts on people (human rights) as well as on the context (conflict)."

[5] We are adopting the EU definition of CAHRA, which defines "conflict-affected and high-risk areas" as "areas in a state of armed conflict or fragile post-conflict as well as areas witnessing weak or nonexistent governance and security, such as failed states, and widespread and systematic violations of international law, including human rights abuses." Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum, and tungsten, their ores, and gold originating from conflict-affected and high-risk areas.

[6] UN OHCHR (2020). "Key Characteristics of Business Respect for Human Rights: B-Tech Foundational Paper."

[7] Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas.

[8] See for example: OECD (2016)."OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas;" EC Commission Recommendation (EU) 2018/1149 of 10 August 2018 on non-binding guidelines for the identification of conflict-affected and high-risk areas and other supply chain risks under Regulation (EU) 2017/821 of the European Parliament and of the Council; UNGA (2020), "Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises Business, human rights and conflict-affected regions: towards heightened action," A/75/212 (hereinafter "UNWG Report, Business, human rights, and conflict-affected regions").

We lay out three distinct eHRDD phases that are supported by stakeholder engagement and industry collaboration:

1 **Creating systems and processes**

Developing a formal eHRDD policy and end-to-end procedure and taking steps to embed eHRDD processes throughout the company as a complement to existing HRDD processes.

2 **Conducting a conflict sensitivity analysis**

Mapping the impact of the company's technology, products, and services on conflict and instability.

3 **Conducting eHRDD**

Conducting additional analysis of new topics and considerations specific to CAHRA, supported by stakeholder engagement and industry collaboration.

What is the aim of this guidance?

This toolkit is intended to help tech companies determine:

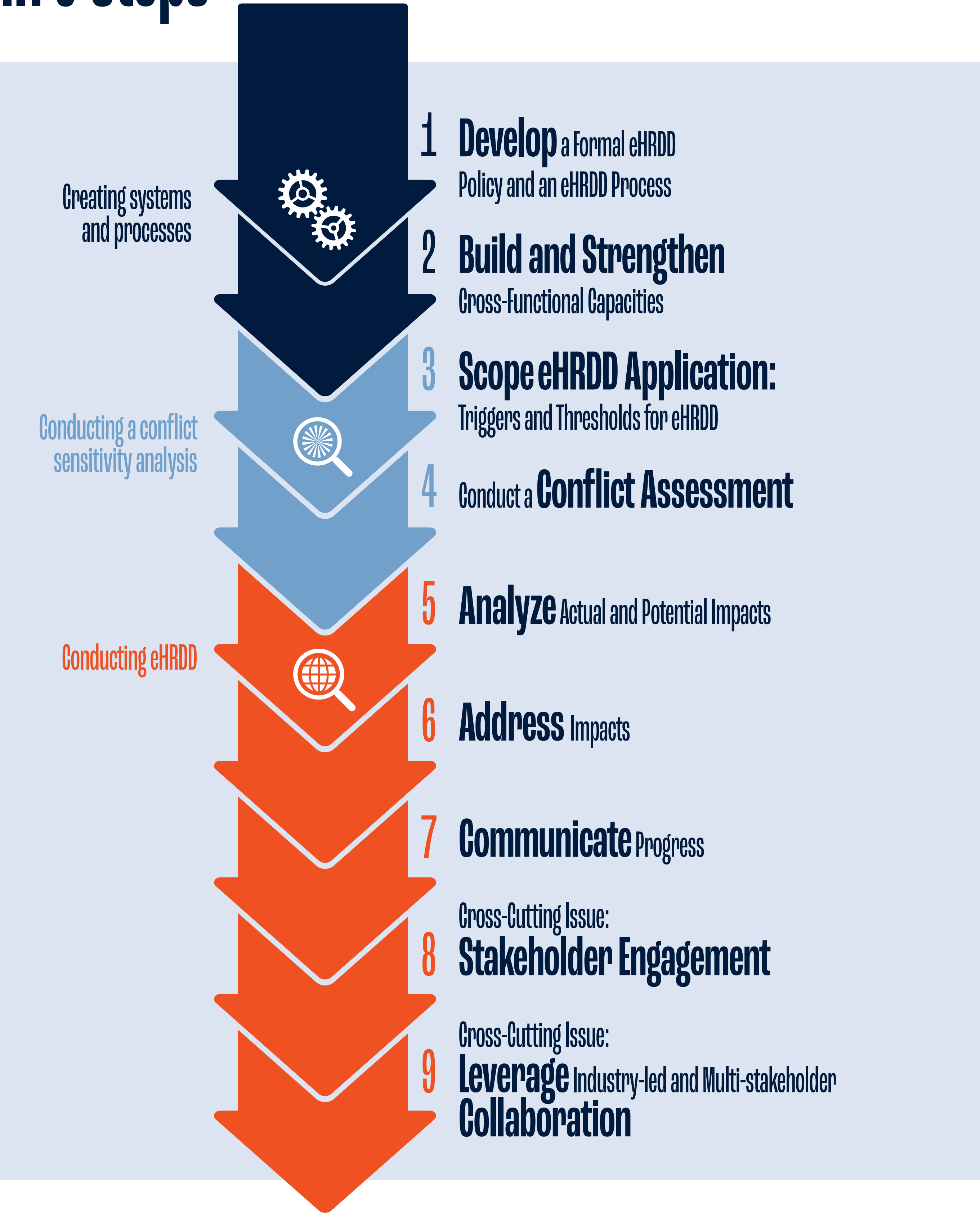
1. **What key systems and processes** they need to have to detect and address human rights risks during conflict;
2. **What situations and contexts** should trigger heightened due diligence practices (including, for example, potential harms, business operations, and the conflict itself); and
3. **What enhanced or heightened due diligence** should entail

Our toolkit provides analytical and operational decision-making guidance for tech companies on navigating conflict-related issues. We've also developed a short Accompanying Primer that summarizes this guidance and can serve as a rapid reference framework for companies as they build out these processes.

The practice-oriented guidance was written in close consultation with both the technology industry and with other diverse stakeholders, including local civil society from high-risk markets.

Practice tip: *Heightened Human Rights Due Diligence for business in conflict-affected contexts is a new UN Development Program guide for conducting enhanced human rights due diligence in conflict-affected contexts. It provides high-level guidance on designing, updating, and implementing corporate human rights due diligence in CAHRA. Grounded in the UNGPs and the work of the UN Working Group on Business and Human Rights, the report should be read as a companion to this toolkit.*

Enhanced Human Rights Due Diligence in 9 Steps



Creating systems and processes

1 **Develop** a Formal eHRDD Policy and an eHRDD Process

2 **Build and Strengthen** Cross-Functional Capacities

Conducting a conflict sensitivity analysis

3 **Scope eHRDD Application:** Triggers and Thresholds for eHRDD

4 Conduct a **Conflict Assessment**

Conducting eHRDD

5 **Analyze** Actual and Potential Impacts

6 **Address** Impacts

7 **Communicate** Progress

8 Cross-Cutting Issue: **Stakeholder Engagement**

9 Cross-Cutting Issue: **Leverage** Industry-led and Multi-stakeholder **Collaboration**

1 Develop a Formal eHRDD Policy[9] and an eHRDD Process

A formal policy for enhanced due diligence in CAHRA will demonstrate the company's commitment to addressing both conflict impacts as well as human rights impacts in high-risk markets.

A public-facing commitment to conducting eHRDD could be included in existing human rights policies.

An internal policy could include more detail on scope, process, and governance specific to eHRDD.

Example: *"We recognize that our products and services may be used in parts of the world facing conflict, instability, and serious human rights harms. We further recognize that the use, misuse, or absence of our products and services in these parts of the world may pose a heightened risk of adverse human rights impacts on users, partners, local communities, and others. To address these potential impacts, we are committed to conducting enhanced human rights due diligence in those areas. We will take appropriate action where we find we are involved with adverse human rights impacts."*

1.1. Base the eHRDD process on existing HRDD processes

A formal eHRDD process—whether standalone or built into existing HRDD processes—will provide consistency and operational guidance that will help move the company to a mature eHRDD process that conducts regular monitoring and ongoing assessments, allowing it to marshal resources and expertise before a developing situation conflagrates into a full crisis or conflict situation.

A formal eHRDD process should be grounded in existing human rights due diligence processes and build upon existing resources, skills, and processes.

A strong eHRDD process will include:

- **Positions and processes** *for scoping, thresholds, and tiering (see below for more on these topics) to determine when a company is dealing with a CAHRA and should apply eHRDD.*
- **A clear procedure and operational guidance** *for eHRDD and a mapping of cross-functional responsibilities, outcomes, governance, and owners for each step.*
- **Regular reviews** *with relevant cross-functional teams where information about potential issues in CAHRA is surfaced, discussed, and addressed.*
- **Escalation processes** *that can address rapidly changing situations; standing up a crisis response team; implementing a "rapid-action channel" for channeling resources to address risks and mitigation actions; and tracking and monitoring impacts, mitigations, and responses.*
- **A specialized stakeholder** *engagement plan and procedure for CAHRA.*
- **Integration** *into regular HRDD processes, such as including CAHRA and eHRDD as standing agenda items in all HRDD meetings, projects, consultancies, hiring processes, etc.*
- **A variety of scalable processes** *and responses depending on the context and the situation's intensity and volatility (see table below).*

[9] As noted in UNDP (2022), "Heightened Human Rights Due Diligence for business in conflict-affected contexts: A Guide." The UN Global Compact provides guidance for companies on how to develop a human rights policy.

Depending on the intensity of the conflict, an eHRDD process should trigger actions such as:

Static, low-intensity conflict	Fragile state with deteriorating democratic institutions and increase in human rights abuses	Volatile, high-intensity conflict
▪ Provide conflict-sensitive feedback on a product, service, or hiring policy. ▪ Conduct an in-depth HRIA on a particular country or product. ▪ Hold occasional cross-functional eHRDD meetings. ▪ Use leverage to advocate with governments or regulators for improved security and human rights. ▪ Conduct regular, on-going in-person stakeholder engagement.	▪ Conduct context-specific conflict assessment and rapid human rights impact assessment. ▪ Hold monthly cross-functional eHRDD meetings. ▪ Based on stakeholder engagement plan, stakeholder engagement leads to planning for additional security measures and alternative engagement strategies as needed. ▪ Establish regular reporting on the context and business operations and decisions. ▪ Plan for contingencies, including escalation of conflict.	▪ Make urgent security provisions for employees and users, suppliers, partners, and stakeholders. ▪ Provide daily security updates for employees and other suppliers, partners, and stakeholders. ▪ Update rapid response impact assessment as the conflict evolves. ▪ Establish crisis response team with daily meetings. ▪ Use third parties and additional high-security measures to conduct stakeholder engagement. ▪ Plan for contingencies, including responsible exit.

Practice tip: *Adjust existing HRDD to build proactive internal capabilities for eHRDD. For example: Ask product teams to flag whether a new product, feature, or service will be applicable to any CAHRA (from the company's CAHRA list, see below), ask sales teams about potentially risky uses of the product or service, or ask the human rights team to flag to a product team when a global change may have specific local impact in CAHRA. This should prompt a product-level rapid assessment about the impacts to the conflict situation, informed by the mapping and analyses explained below.*

Engage in futures methodologies and case studies, conduct scenario planning exercises, and develop playbooks of response protocols for likely and high-risk events.

1.2. Plan for contingencies

Hold crisis scenario or conflict-related tabletop exercises to engage with different teams and align on necessary resources to plan for and respond to conflict contexts. Get diverse teams thinking about how conflict settings are different from "standard" due diligence settings.

Conduct internal workshops around positions in conflict settings and where they might need to shift from existing values and positions on human rights. Ask:

- *Can this eHRDD process be done consistently, globally, in all similarly situated conflict situations?*
- *What is our risk tolerance and capacity for mitigations in conflict settings? Is it different from other non-CAHRA contexts where the same rights might be at issue?*
- *Do we need to adjust our positions about priorities, mitigations, and "exit" or termination, considering the company's impact on conflicts and related human rights?*

A note on HRIAs in CAHRA: *For high-risk markets, full-scale HRIAs may not be the best response to rapidly emerging risks. Timelines are too short, and impacts are too serious.*

However, HRIAs are strongly recommended for specific products and services and their potential impact on conflict as a specific subject as a preventative, baseline-setting exercise. These will be invaluable tools in developing playbooks for potential responses and understanding the dynamics of how individual products and services influence conflict at a general level, to be then used and tailored to individual contexts as the need arises.

2 Build and Strengthen Cross-Functional Capacities

Conflict situations may require engaging with different teams that are not always involved in HRDD. Consult regularly with or expand existing working groups and committees to include representatives from other relevant verticals in the company, to surface and discuss potential and ongoing risks in conflict contexts (see the "Toolbox" on page 39 for examples.)

Benefits to this approach include:

- *Development of timely rapid response plans across teams to address high-risk situations.*
- *Integration of eHRDD principles into more mature due diligence processes in other teams (such as financial crime risk management, integrity teams, procurement, etc.). This can help them enhance their own due diligence, risk prioritization and tiering.*
- *Alignment on risk appetite, necessary resources to plan and respond, and getting diverse teams thinking about how conflict settings are different from "standard" due diligence settings.*
- *Break-down of internal siloes, promoting an integrated approach to eHRDD in conflict contexts.*

2.1. Leverage existing teams and capabilities

Cross-functional teams' expertise and resources should be leveraged to strengthen eHRDD processes. Include these teams in periodic human rights steering committee meetings and workshops on individual issues of concern to that team.

Practice tip: *Cross-functional teams' ability to detect nuanced risks in conflict settings will increase if they are provided clear trigger or triage questions. A tool for this is provided in the "Toolbox" on page 39.*

2.2. Build eHRDD capacities across teams

Build eHRDD processes and conflict impacts into human rights or other relevant training, such as those for content moderators. Training should be tailored to the specific situations that these employees will confront. An employee responding to user complaints about their content being removed in a rapidly changing conflict context will need different resources and support to make a conflict-sensitive decision than an executive weighing whether to pursue a new business venture in a CAHRA market.

3 Scope eHRDD Application: Triggers and Thresholds for eHRDD

3.1. Establish criteria for when to apply eHRDD

eHRDD is needed in a variety of contexts and situations. Factors that should trigger eHRDD include:

Situation	Triggers
Market-entry	▪ The country is in the midst of an on-going conflict (local or national) or the situation is rife for a conflict (e.g., state of emergency, simmering tensions that frequently spill over). ▪ Conforming with the regulations and directives of the ruling government is likely to lead to violations of human rights and heightened conflict. ▪ Vulnerable users of the technology (e.g., journalists and human rights defenders) are likely to face cyber-attacks from malicious conflict actors.
Release of a new product / service or feature / functionality	▪ The product or service is likely to be used or misused by conflict actors (e.g., the government or armed militia) to create conditions that heighten conflict. ▪ New product features could increase security vulnerabilities that are exploited by conflict actors.
Policy management, release, and implementation, such as content moderation policies or data release request processes, including any changes	▪ Consistent enforcement of policies across all sides of a conflict is unlikely and could result in an altering of power dynamics that exacerbates conflict.
Office opening / meeting presence requirements	▪ The company could become "captive"[10] to a conflict actor (e.g., the government) and be forced to comply with overly broad local interpretations of license agreements and / or local law by the government (e.g., around national security arrangements or content moderation). In exceptional circumstances, a company could be forced to cede operational control, especially if it provides a crucial service (e.g., telecommunications). ▪ The safety and liberty of company personnel is likely to be threatened.
Changes in contexts where a company has existing business activities or supply chains	▪ There is a significant deterioration in the rule of law situation in the country, resulting in significant threats to life and liberty of civilians: • *Government regulation that unduly limits free expression or seeks increasing access to users' personal data.* • *Orders for internet shutdowns that do not meet international standards.* • *Violence and harassment of certain groups based on their identity, including through the use of digital tools.* • *Arbitrary detentions of human rights defenders, advocates, and journalists for legitimate online speech or other activities in the digital realm.*

Practice tip: *Evolving regulations may create situations where eHRDD is legally mandated. For example, the European Commission has proposed the creation of a "crisis mechanism" through the Digital Services Act (DSA). Applicable in public health or security crises, the Commission, or any of Europe's 27 member states, could require large tech companies to take steps to address adverse impacts of their activities on the crisis at issue.*[11]

[10] The concept of "captive" businesses has been detailed in the UNWG Report, "Business, human rights, and conflict-affected regions."
[11] See, e.g., Arturo J. Carrillo, "Between a Rock and a Hard Place."

3.2. Develop a list of relevant CAHRAs

Develop a list of CAHRA markets and operating contexts. This list will be used to identify markets where eHRDD is needed. Factors that should put a market on your list include:

- *Existence of international armed conflict, non-international armed conflict, or other forms of war and widespread violence*
- *An occupied or disputed territory, or occupied populations*
- *Widespread human rights abuses, including civil rights abuses*
- *Weak rule of law*
- *Non-democratic governments, autocracy, or abusive regimes*
- *Regional conflicts*
- *Economic pressures from climate change*
- *Destabilization from trading partners and other geo-political indicators of instability*
- *Situations that are escalating and moving into a potential conflict scenario*
- *Changes in conflict intensity and worsening human rights contexts in protracted conflicts*

See the "Toolbox" on page 39 for a list of useful external sources for this.

3.3. Define parameters for eHRDD by gathering internal data on relevant markets and business activities

Internal market-based data can be diverse and are largely used to help provide a quick high-level indication of the scope of a company's potential impacts on a conflict or human rights. Such indicators are included in the "Toolbox" on page 39.

Contexts where there are ***severe*** *conflict and human rights impacts should still be resourced and addressed with eHRDD,* ***even if*** *there is minimal or no official market share.*

3.4. Conduct proportionate risk tiering of CAHRAs

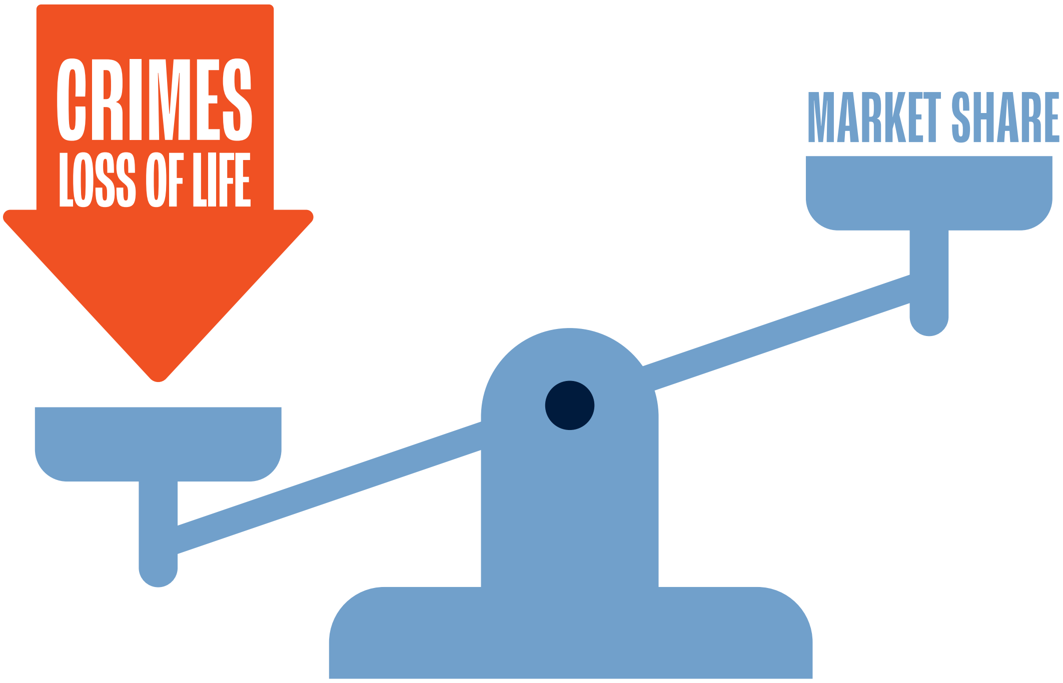
Once a list of CAHRA is created, taking a risk-based approach to prioritizing areas for eHRDD is appropriate. This will help proportionately target resources and responses to the CAHRA that pose the biggest risks to conflict and human rights.

Practice tip: *When risk tiering and planning for escalations, be sure to consider internal constraints and planning cycles. In short, don't spend all available time and resources on higher risk tiers. Medium-risk contexts and low-risk contexts can quickly escalate; ensure a base level of preparation and diligence has been conducted in advance.*

Risk tiering will impact available resources for addressing conflict risks and the scope of potential mitigations. It needs to be nuanced and well-informed and should include both quantitative and qualitative data.

Quantitative Data	Qualitative Data
▪ Conflict intensity (battle deaths); ▪ Regions impacted; ▪ Internal data on users; ▪ Market penetration; ▪ Risk tiering results from other internal teams (e.g., Security, Trust & Safety, Financial Crimes, Legal, etc.); ▪ Scores from various human rights indexes.	▪ Conflict intensity (political analysis); ▪ Conflict actors; ▪ Historical grievances and other conflict drivers; ▪ Vulnerable groups; ▪ Salient human rights impacts that arise due to the conflict, and impact of products and services (as distinct from pure market penetration or financial recovery); ▪ Feedback from local stakeholders.

IN CAHRA, HOW INDICATORS ARE **WEIGHTED** MAY NEED TO BE ADJUSTED.



Normal HRDD risk tiering is based on severity (which in turn includes analyzing the scale, scope and remediability of an adverse impact) and likelihood of harm. Risk tiering for prioritizing eHRDD in CAHRA requires different considerations than in normal HRDD, including an assessment of impact on the conflict in addition to human rights impacts. Stakes are higher—lives are often at risk—and timelines can shorten as conflict escalates.

In CAHRA, how indicators are weighted may need to be adjusted.

For example:

- *Market share or user-base may need to be weighted less—it is a less determinative factor—where potential human rights impacts are especially grave. Contexts where there are severe conflict and human rights impacts should still be resourced and addressed with eHRDD, even if there is minimal or no official market share.*
- *Indications of atrocity crimes or serious loss of life should be heavily weighted.*
- *Scope of impact of products or services may need to be adjusted based on context; for example, where they play an outsized role in the conflict, consider a higher risk tier.*
- *Companies need to be careful not to limit their scope to users or customers. In some cases, the scope could be entire populations.*

Practice tip: *Decisions on how to weigh these factors will often require internal alignment. Conduct workshops and risk-appetite conversations with internal stakeholders and cross-functional teams to discuss different situations of risk, such as:*

Risk Profile	Hypothetical Situation
A low likelihood of risk but the risk itself is very high, such as severe and irremediable harm or risk to life.	An employee is sent to repair company infrastructure in a part of the country experiencing a flare-up of violence. The employee's gender or ethnicity makes her a target of violence.
A high likelihood of risk but the risk itself is of low severity—but can impact power dynamics of a conflict setting over time.	Consistently over-enforcing a content moderation policy on one side of a "static" conflict and under-enforcing it on the other. The immediate impact of the action is not severe, but over time, cumulative impacts could lead to influencing power dynamics between conflict actors and exacerbating the scale of the conflict.
A likely serious risk of harm to communities that use a company's free products and services in a country that is in active conflict but is not considered a formal "market" for the company.	A country in conflict is not identified as a formal "market" for the company but its products and services are freely available there. Lack of recognition as a formal market leads to under-resourcing which increases the likelihood of large-scale harms to communities.
A high likelihood of serious risk of cumulative harms to communities that use a company's products and services in a country that is experiencing increasing tensions and increasingly authoritarian government practices.	A government orders internet shutdowns in a restive region of the country. As an immediate impact, rightsholders experience a restricted right to access and share information and to communicate. Cumulative impacts lead to an inability to organize political action, share warnings or evidence of attacks or atrocity crimes, work, go to school, or access health services.
A high likelihood of severe and immediate risk to a small number of users in a CAHRA.	Users of a platform or service in a CAHRA are at risk of being targeted by authorities based on data shared through a formal Law enforcement request (LER). The market share is low, but leads to disappearances and deaths of users who are targeted.

These conversations and the resultant risk models can help build predictability, defensibility, and more efficient resourcing into the planning and response. See the "Toolbox" for a sample risk card.

3.5. Establish and maintain a system for monitoring new CAHRAs, updating risk tiers, and escalation procedures

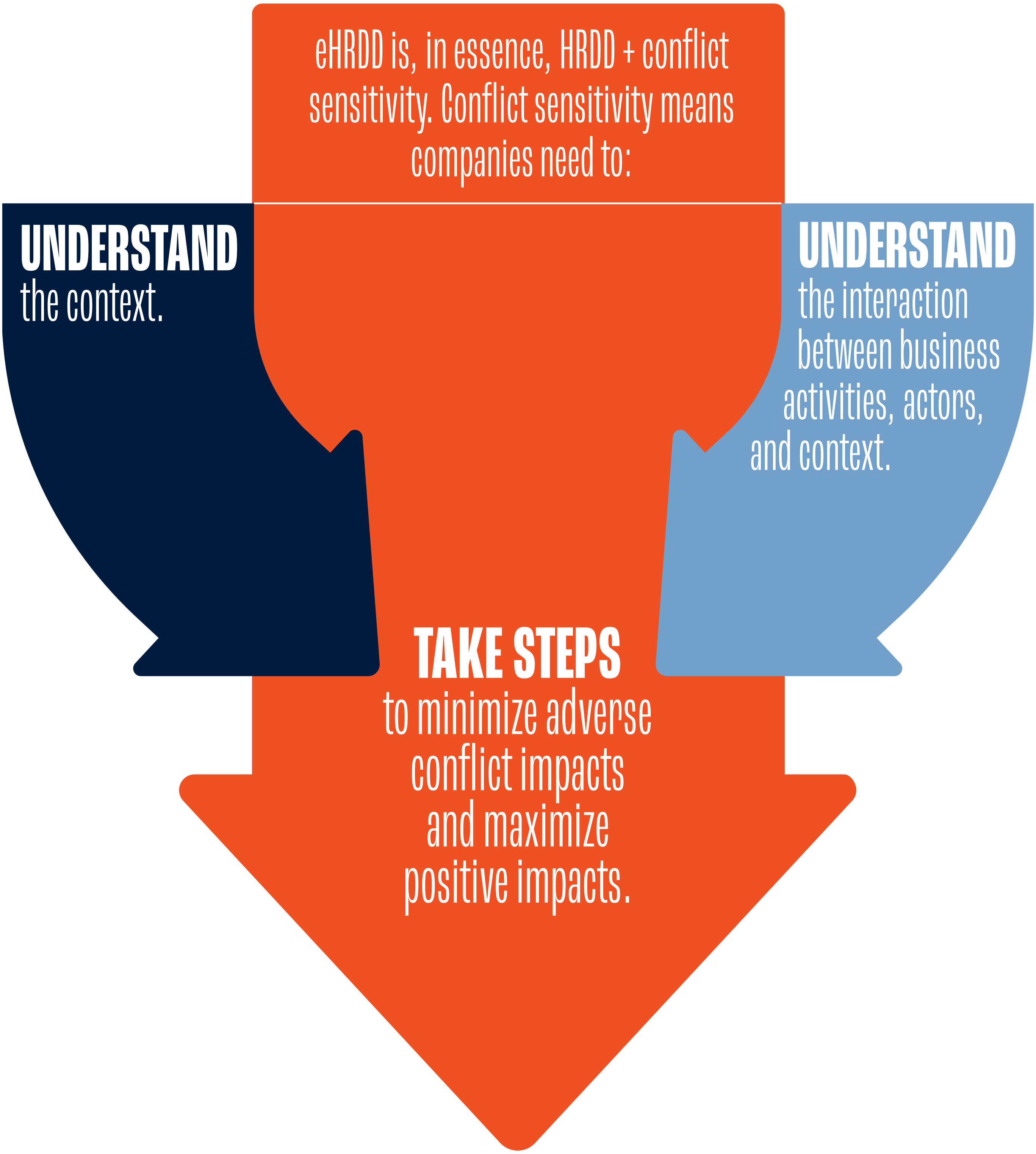
Conflicts operate in a cycle. Establish a process for monitoring new CAHRAs and updating the CAHRA list based on the steps included above. The list should be regularly maintained and thoroughly assessed at least quarterly.

Risk-tiering should be reviewed and adjusted frequently in CAHRA situations. Review risk tiering for stable conflicts quarterly, and more frequently—at least monthly—as the situation warrants. If the risk tiering process is automated or heavily quantitative, increase the frequency of review.

Establish or update escalation procedures to ensure that senior executives are kept apprised of changing situations through existing channels.

Practice tip: *External risk firms can be useful to help flag emerging crises and conflicts. Security teams may also use external vendors for assessing risk. Align with internal teams and external vendors on factors used for identifying risks and ensure that conflict and human rights risks are both included.*

4 Conduct a Conflict Assessment



eHRDD is, in essence, HRDD + conflict sensitivity. Conflict sensitivity means companies need to:

UNDERSTAND the context.

UNDERSTAND the interaction between business activities, actors, and context.

TAKE STEPS to minimize adverse conflict impacts and maximize positive impacts.

4.1. Understand the context

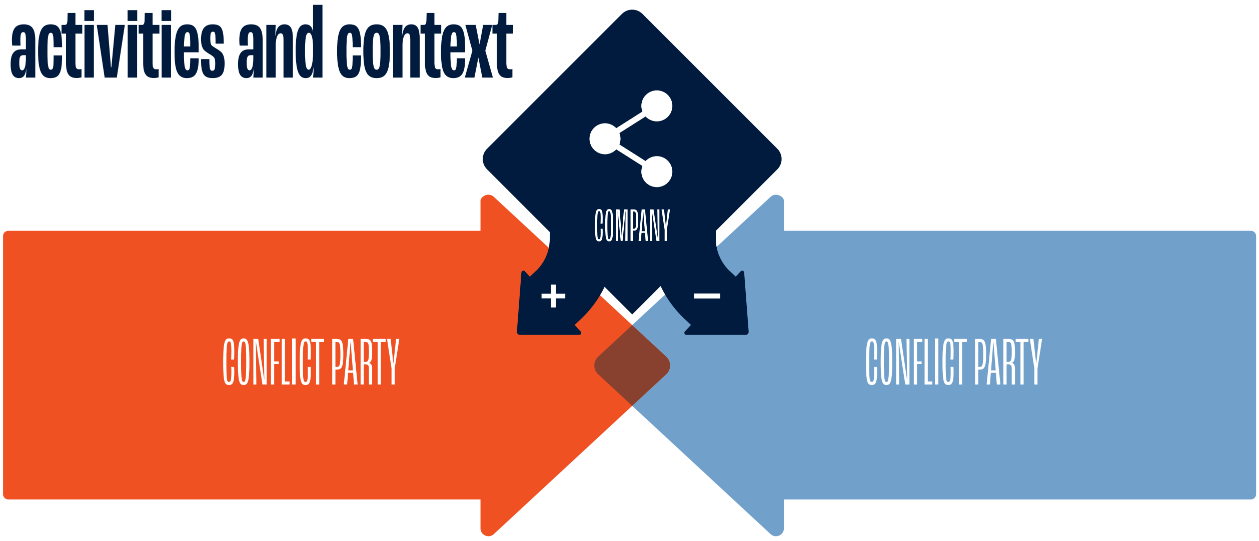
For any situation included on the high-risk market list and therefore subject to eHRDD, additional research needs to be conducted to provide an understanding of the conflict. The UNDP's Conflict and Development Analysis Tool provides detailed guidance on conducting conflict analysis and applying the findings of analysis for a range of purposes.[12] Adapting the UNDP tool to a technology company operating in conflict, conflict assessment steps could look like the following:

Step	Key Activities
Situation analysis	Analyze the current situation vis-à-vis the conflict to develop a baseline understanding and highlight issues for deeper consideration: ▪ What is the current state of the conflict? ▪ What is the existing situation regarding: • *internal security* • *geopolitics* • *rule of law and human rights* • *economic situation* • *condition of minorities and vulnerable groups?* ▪ Is the conflict regional, international, internal, or localized to certain states within a country?[13]
Factor assessment	Identify "conflict factors." These include underlying or longstanding causes related to systemic inequalities as well as more proximate causes like a drought or election. These will be particularly important when understanding hiring decisions, potential office locations, general terms and conditions, or language requirements for content moderation decisions: ▪ What are the long-term root/structural issues of the conflict ("Root factors")? ▪ How does the conflict visibly manifest ("Proximate factors")? ▪ What events/issues could lead to further exacerbating of the conflict ("Triggers")?
Stakeholder analysis	Identify, map, and analyze the key actors in the conflict. Within the UNDP CDA framework, the term "actors" refers to individuals, groups, and institutions engaged in—and affected by—conflict. They may not be located in the CAHRA but can be external influences or part of the diaspora. These can be online and offline actors, and their behaviors may be different based on that factor. ▪ Who is fighting who, and why? How dangerous are they? ▪ What are important relationships to monitor? ▪ What are divisive factors in this situation? What issues cause disagreement or hostility among conflict actors? ▪ How does this play out online, and how is it different from offline behaviors?
Understand conflict trends (see S 4.2 for more detail on this)	**Based on the above analysis, identify "conflict drivers" and "peace engines" to understand conflict trends and patterns:** **Conflict drivers:** "are dynamic processes that contribute to the ignition or exacerbation of destructive conflict." They are often a combination of the "conflict factors" described above and could include: ▪ How are organized groups convening online to plan and target vulnerable groups? ▪ Which groups are they targeting and how? ▪ What role is the government playing here? **Peace engines:** are elements that "mitigate the emergence and proliferation of violent conflict." They can take the form of institutions, groups, individuals, processes, symbols, or social constructions. ▪ What are the things that bring people together or have the potential to de-escalate tensions? ▪ Where do people meet or come together—is it online, through chat services, or social media?

[12] See UNDP (2017). "Conducting a Conflict and Development Analysis."

[13] Sometimes very region-specific violence and conflict can spill over internal and even international borders. Sometimes contexts or crises are by nature cross-border, such as terrorist activity in West Africa or refugee crises. These cross-border dynamics and contexts will require further analysis, including with respect to local language-support and potential geo-political or historical grievances at issue.

4.2. Understand the interaction between activities and context



Understand how company operations, staff, policies, practices, services, or products could impact the conflict itself, in addition to human rights. Companies can impact conflicts in many ways, including through its specific products, services, and business models, as well as through its actions, omissions, resources, behaviors, and messages. This includes local and international staff. Key categories of questions for consideration include:

- **Product use:** *Are the company's products and services used disproportionately more or exclusively on one side of the conflict | grievance? Do vulnerable groups have access to the company's products and services?*
  - *How are the different actors in this conflict (including communities and individuals) using products, services, infrastructure, or other aspect of the business?*
  - *Why are they using this product or service? Is there a particular feature or aspect of it that facilitates misuse in this context (e.g., end-to-end encryption, local regulatory powers facilitate access to data, broad user-base among supporters, etc.)?*
  - *Does that use conform with their obligations under IHL, if IHL is applicable in this context? (For example, does it violate human rights, is it proportionate, does it facilitate unlawful attacks against civilians, etc.?)*
  - *Does that use increase a conflict-actor's position with respect to the conflict? (For example, does it provide access to data sources, facilitate unlawful attacks on civilian populations, block access to information or communications, promote violence among supporters or against rival groups, etc.?) Do content moderation policies impact conflict-affected communities or exacerbate historical grievances or systemic vulnerabilities?*
  - *How does that use relate to any conflict grievances?*
  - *How does that use impact vulnerable groups? Does it put additional groups at risk of harm? Does the use disproportionately impact women and girls? (See Section 5.2 below on different types of potential impacts)*
- **Business relationships, procurement, and hiring:** *Are the company's operations, products, or services linked to any business relationships of conflict actors? By engaging with certain conflict actors, or their business relationships, is the company legitimizing, strengthening, or enabling them? Are procurement and hiring practices providing financial resources to particular groups of people?*
- **Government access to data, tools, and infrastructure:** *Will complying with government requests for data enable or facilitate human rights violations by the government or military? Is it likely that a company's products would be used for illegal targeting decisions? Is it likely that a company infrastructure would be used by militias or military?*
- **Harmful content targeting specific groups:** *Are social media channels being used by powerful actors to incite violence or hate crimes against specific groups? Could algorithms spread hate speech or misinformation? What groups are targeted, and how does it impact conflict dynamics, including long-standing grievances?*

- **Is the company enforcing policies equally or to equal effect among conflict actors?** *Is there any potential bias in the practical application of policies and procedures? Can disparate impacts of policy enforcement alter the balance of power of conflict actors?*
- **Security threats targeting vulnerable groups:** *Will human rights defenders, political opponents, or other targeted groups be at risk if they have accounts or due to their content on the platforms? How could the company's products or services be used in cyberattacks or hacking attempts against these groups?*
- **Obstacles to conflict resolution:** *Will company actions or mitigations make it harder for people to come together against conflict actors or strengthen those who exacerbate conflict? Could company actions, omissions, or mitigations impede accountability or transitional justice efforts or the creation of alternative narratives about the conflict by deleting potential evidentiary content, facilitating official denial of events, or influencing the reach of diverse views about events?*
- **Risks pertaining to local staff:** *Will staff be at risk if asked to enter a certain part of the country based on their ethnicity or perceived alliances? If the company rejects a government or militia request because it negatively impacts the conflict, will staff or their families be put at risk? Will the ethnicity and background of local staff add to conflict grievances or perceptions of bias?*
- **Societal impacts:** *Is the company partially or fully replacing existing societal or state functions, systems, or structures? How might company activities affect the positions of power or relationships between different actors? Do company activities influence conflict actors' access to sources of data, amplify their messages, or facilitate their warfare?*

4.3. Assess International Humanitarian Law

For all CAHRA countries where international humanitarian law applies (including Occupied Territories, Non-International Armed Conflicts, and International Armed Conflicts),[14] conduct a legal assessment to identify the company's legal obligations and the obligations of other stakeholders.

International human rights law and international humanitarian law apply simultaneously in situations of armed conflict (both international and internal) and in situations of military occupation.The UNGPs note that conflict may increase the risk of a business being complicit in human rights abuses committed by other actors (e.g., a military government). For this reason, companies are required to respect international humanitarian law and should "treat the risk of causing or contributing to gross human rights abuses as a legal compliance issue wherever they operate."[15]

International Human Rights Law (IHRL)	International Humanitarian Law (IHL)
According to the ICRC, "IHRL is a set of international rules, established by treaty or custom, on the basis of which individuals and groups can expect and/or claim certain behavior or benefits from governments. Every person, simply as a consequence of being human, has certain basic entitlements: these are called 'human rights.' Numerous non-treaty-based principles and guidelines ('soft law') also belong to the body of international human rights standards."	*According to the ICRC, "IHL is a set of rules that seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or who are no longer participating in hostilities, and it restricts the means and methods of warfare. IHL is also known as 'the law of war' or 'the law of armed conflict.'"*[16]

[14] For more on the typology of armed conflict and IHL, see Sylvain Vité, "Typology of armed conflicts in international humanitarian law: legal concepts and actual situations", IRRC 873 (2009).

[15] See UN Guiding Principle 23 and related commentary.

[16] ICRC (2017), "Recent developments of the interplay between IHL and IHRL." For more on the differences between these two bodies of law, see ICRC (2015), "What is the Difference between IHL and human rights law?“

This is especially crucial if their activities are "closely linked" to the conflict (i.e., "if they provide direct support—be it military, logistical, or financial assistance—even if they do not take place during actual fighting or on the physical battlefield and even if the business did not actually intend to support a party to the hostilities.")[17]

In very limited circumstances, a state may lawfully suspend some of its derogable human rights obligations.[18] If state practices and directives conflict with human rights, tech companies should understand the extent of the conflict by carefully examining the rules, seeking clarification from the government, and pushing back against unreasonable demands (while also assessing the risks to any staff in carrying out these actions).[19] They should also test their approaches with local stakeholders and experts, working collaboratively with other companies to strengthen leverage. A thorough IHL assessment can help a company better understand its obligations and prevent it from worsening a situation. Additional guidance on mitigation measures is provided below.

4.4. Take steps to minimize adverse impacts and maximize positive impacts

The information based on the previous analysis will be used in risk tiering, impact assessments, and mitigation planning, all discussed below.

5 Analyze Actual and Potential Impacts

This step enables companies to create a prioritized list of the company's salient human rights risks, created through a conflict-sensitive approach to human rights salience assessment and prioritization. The conflict analysis should inform this process. It is worth emphasizing here that impacts are analyzed from the perspective of the rightsholders—that is, the people or peoples experiencing the adverse human rights impacts.

5.1. Identify vulnerable groups

Identify groups or individuals that are vulnerable in high-risk markets, and who therefore may need special accommodation or protection.[20]

These vulnerable groups may be disadvantaged, marginalized, or excluded from society in several ways, including through:

- *Formal discrimination (e.g., by laws and policies);*
- *Societal discrimination (e.g., through cultural beliefs or taboos);*
- *Practical discrimination (e.g., access barriers for people with disabilities); and*
- *Hidden discrimination (e.g., individuals who cannot reveal their identity, such as LGBTQI+ individuals).*

[17] "Australian Red Cross and RMIT University (2020), "Doing Responsible Business in Armed Conflict: Risks, Rights, and Responsibilities," as cited in the UNWG's 2020 report on "Business, human rights and conflict-affected regions: towards heightened action."

[18] Note that the issue of suspension of certain rights during conflict is a debated area of law and is context-dependent—the context being different with each request or interaction. The ICRC recommends adopting a case-by-case approach to determining which body of law applies in each situation.

[19] Rachel Davis, International Review of the Red Cross, V. 94 No. 887 (2012), "The UN Guiding Principles on Business and Human Rights and conflict affected areas: state obligations and business responsibilities."

[20] BSR has developed a framework for assessing vulnerability, based on the UNGPs.

Vulnerability is context dependent and can change depending on conflict dynamics. Build an understanding of local identity politics, grievances over perceived and actual discrimination, minority group identity, cultural practices, religion, and life circumstances.

Use broad sources of information, including stakeholder engagement, as well as reports from women's organizations and indigenous groups.

Practice tip:

Pay particular attention to women and girls, who are disproportionately affected by conflict and who are at risk of sexual violence, as well as human rights defenders, who are frequently targeted with physical and legal harassment in markets where there are poor human rights protections for rights like freedom of expression, information, and association. Understand how the conflict can change vulnerabilities and social relationships, and how the use of the company's products and services may do the same.

5.2. Identify conflict and human rights impacts

eHRDD processes should examine how business activities impact existing tensions, conflicts, and power dynamics by integrating the conflict analysis. This process is based on the assessment of how the company interacts with conflict dynamics, moving from generalized interactions to specific impacts.

Impacts should be considered holistically, across communities, and should also include cumulative impacts and "second order" or "knock-on" impacts (e.g., internet shutdowns can have secondary impacts of loss of income and information). Note that sometimes these harms can extend beyond borders.

Consider actual and potential impacts.This is where the conflict assessment (as described in section 4 above) will be helpful.

The following questions can help identify these impacts:

- *How are the different actors in this conflict (including communities and individuals) using our products, services, infrastructure, or other aspect of our business?*
- *Why are they using this product or service? Is there a particular feature or aspect of it that facilitates misuse in this context (e.g., end-to-end encryption, local regulatory powers facilitate access to data, broad user-base among supporters, etc.)? Does that use conform with their obligations under IHL, if IHL is applicable in this context (e.g., does it violate human rights, is it proportionate, does it facilitate unlawful attacks against civilians, etc.)?*
- *Does that use strengthen a conflict-actor's position with respect to the conflict (e.g., provide access to data sources, facilitate unlawful attacks on civilian populations, block access to information or communications, promote violence among supporters or against rival groups, etc.)?*
- *Do our content moderation policies and their implementation impact conflict-affected communities or exacerbate historical grievances or systemic vulnerabilities?*
- *Are our existing financial crime risk management or anti-corruption processes a source of risk (e.g., by leading to over-enforcement of anti-money laundering rules)?*
- *How does that use relate to any conflict grievances?*
- *How does that use impact vulnerable groups? Does it put additional groups at risk of harm? What are the potential harms to vulnerable groups as a result of this use?*

Categorize impacts by immediate, future, and cumulative depending on when they will likely occur.

Examples could include:

Immediate impacts:

- » *Physical harm or loss of life from a social media campaign calling for indiscriminate attacks or attacks against a particular ethnic group.*
- » *Use of products and services for government surveillance in violation of international human rights law norms causing immediate privacy and bodily security impacts (i.e., to locate, arrest, and imprison someone).*
- » *Loss of access to information from an internet shutdown.*
- » *Violation to the right to privacy from government data requests.*
- » *Loss of right to participate in public life and | or government.*
- » *Harassment of local staff if company refuses to comply with government requests (this could include violence, destruction of property, arbitrary detentions, lawsuits, and similar acts of intimidation).*
- » *Doing business with suppliers and local vendors who are affiliated with conflict actors.*

Future impacts:

- » *Use of products and services for government surveillance in violation of international humanitarian law norms causing future impacts associated with an expanded government surveillance state on collective privacy violations.*
- » *Violence against an ethnic group fomented on social media leads to:*
  - Internal displacement and cross-border refugee crisis
  - Regional destabilization and increased insecurity
- » *Loss of access to information from an internet shutdown or over-moderation of content leads to:*
  - Loss of work and income
  - Loss of education, access to healthcare, and/or access to financial services
  - Inability to vote or participate in elections
- » *Violation of the right to privacy from government requests leads to:*
  - Attacks on human right defenders
  - Arbitrary arrest and torture
  - Increased systemic attacks and oppression against rival groups based on insights gleaned from data

Cumulative impacts: Any of the above can build into cumulative impacts, such as:

- » *Increased state fragility and security more broadly, including loss of right to self-determination and political participation.*
- » *Loss of economic opportunities, food security, and health, including impact on a variety of economic and cultural rights.*
- » *Deepening social polarization and inter-communal violence, including scarcity of resources as a result of conflict.*

Using the above methodology, a sample set of "Conflict and Human Rights Impacts" could include the following:

- *Deepened grievances that prolong the conflict (actual impact, immediate, cumulative)*
- *Destabilizing democratic systems of government and promoting authoritarianism (actual impact, future, cumulative)*
- *Loss of opportunities for accountability and transitional justice (potential impact, future, cumulative)*
- *Spreading the conflict throughout state territories and the region, shifting geo-political responses to the conflict (actual impact, immediate, cumulative)*
- *Detracting from peacebuilding opportunities (potential impact, future, cumulative)*

Note: To take a truly "conflict sensitive" approach, companies should also identify and understand opportunities to positively impact the conflict and take steps to augment those opportunities.[21]

Practice tips:

- *Conduct this analysis in a "gender-sensitive"[22] way and ensure it reflect the needs of vulnerable groups.*
- *Be careful not to equate "conflict" and "risk." Certain environments have lots of conflict, but tech companies may play a relatively small role there (possibly due to lack of penetration) resulting in lack of salient human rights risk. Other contexts may be relatively peaceful but companies may be involved in significant negative human rights impacts. Also, recall that "risk" refers to risks to rightsholders and the conflict itself, not risks to the company.*
- *Ideally, risks should be identified locally and not at headquarters. This will be more likely if human rights risks form part of the ERM process. However, it may be difficult for a local team to manage these risks if they are already embroiled in a crisis. In addition, the headquarters should be aware of and take steps to address potential bias among local employees. Function-specific human rights training is a helpful way to support local teams' ability to capture and manage emerging crises, potentially with the help of external experts.*

5.3. Assess salience (severity and likelihood) of impacts

Like standard HRDD, eHRDD requires companies to assess the salience of conflict and human rights impacts according to severity and the likelihood of an adverse impact. While assessing salience, the company should assess the impact of its actions and omissions against all core human rights, resulting in a list of key human rights risks.[23] In CAHRA, companies should evaluate the impacts on the conflict separately (see Section 4.2), and use the conflict impacts assessment to inform the assessment of human rights impacts.

For assessing salience, we recommend following the methodologies prescribed by B-Tech and BSR, which are based on the UN Guiding Principles. The steps below, build on the processes detailed there. The questions below focus more on the impacts arising out of misuse of a technology product (e.g., a social media platform), and will be different while assessing salience during market-entry, changes in context, infrastructure, or office presence in the region.

[21] Resources by organizations such as PeaceTech Lab, Alliance for Peacebuilding, the Toda Peace Institute, Mercy Corps, Search for Common Ground and Build-Up are worth examining in this context.

[22] The UN has provided a framework for applying a gender lens to the UNGPs. The UN's conflict analysis tool also provides a series of indicators for assessing the unique impact of conflict on women (page 58 onward).

[23] The baseline here being the International Bill of Human Rights coupled with the principles concerning fundamental rights in the eight ILO core conventions as set out in the Declaration on Fundamental Principles and Rights at Work.

Step	Indicators
Scope: How many people could be affected by the adverse impact?	How widespread are the violence or conflict activities resulting from use of the technology? Which groups are most adversely impacted and how? ▪ Do these include vulnerable groups such as women, children, LGBTQI+, people with disabilities, ethnic and religious minorities? ▪ Do these include journalists and human rights defenders? Why are these groups being targeted? **Note:** *Companies need to be careful not to limit their scope to users or customers. In some cases, the scope could be entire populations.*
Scale: How serious are the adverse impacts for the victim?	Are people losing their life or facing physical violence? Are people being intimidated through arbitrary arrests and lawsuits? Are people living under fear resulting in self-censorship and use of tools to conceal their digital footprint?
Remediability: Will remedy restore victim to the same or equivalent position before the harm?	Is remedy feasible in this context? Can impacted individuals or communities be made the same, or equivalent to, their situation before the armed conflict, oppression, or violence escalated? What would remedy look like for different victim groups?
Likelihood: How likely is it for the impact to occur?	What are user interests, motivations, and incentives? Is there an interest in using or misusing the product or service in a way that exacerbates conflict? Or as a weapon? What is the user's technological capacity? Will a user's technological capabilities, or lack thereof, make it more or less likely that the conflict impacts will occur? Are there any technical barriers, such as access to computing power, electricity, servers, or internet, that will make the use-case unlikely in practice? Are there government policies and laws that will make the use case more or less likely in practice (such as on mandatory data sharing or crisis-related content-moderation policies)?

A risk scale in the "Toolbox" section provides a practical, quantitative way to measure salience.

Practice tips:

- *Build off established Know Your Partner or Know Your Customer due diligence to support this analysis. Focus on issues that are relevant to conflict or human rights, such as relationships to military or government, armed groups, and other conflict-related business relationships; use-cases likely to adversely impact vulnerable groups; or business models or supply chains that pose high risk of adverse conflict or human rights impacts.*
- *Integrate these risks into the Enterprise Risk Management framework, to inform strategy, human rights risk registers, and to identify risks to enterprise value.*[24]

Note: CAHRA are complex and frequently change and there will be some subjectivity and uncertainty in this analysis (which can be mitigated by robust stakeholder engagement). While companies may not be able to completely assess all risks through this analysis, they are expected to "take all reasonable steps to achieve an analysis based on the available facts, intelligent foresight, and sound judgment." [25]

[24] BSR (2021). "Human Rights Assessments: Identifying Risks, Informing Strategy."

[25] UN OHCHR (2020). "Identifying and Assessing Human Rights Risk Related to End-Use: A B-Tech Foundational Paper."

5.4. Conduct proportionate risk tiering of impacts

Once a list of salient risks has been developed, the next step should be to tier them according to priority. Priority is determined by severity and likelihood. Other factors (see the sample risk matrix in the "Toolbox"), including attribution and leverage, should help companies determine the appropriate action. Tiering specific impacts in CAHRA requires different considerations than in normal human rights contexts.

5.5. Examine attribution

The cause-contribute-(directly) linked framework can help companies determine their attribution to a human rights harm. It is not an exact determination and should be used as a tool to help guide response (e.g., is a specific internal change to be prioritized or is a more systemic response appropriate?) rather than constrain action.

OHCHR's B-tech project provides a useful framework for helping determine a tech company's attribution to harm. The steps below are based on those recommendations and include additional considerations for CAHRA and eHRDD processes.

Attribution	Explanation	Example	Recommended Action
Cause	The **company's activities** (actions or omissions) on their own "remove or reduce a person's (or group of persons) ability to enjoy a human right." For CAHRA, this would extend to an analysis of whether a company's activities or omissions exacerbate or worsen conflict dynamics or contribute to conflict drivers.	Social media company censoring legitimate speech, to prevent fallouts with powerful conflict actors (e.g., an authoritarian government). **Ask:** Is the company actively supporting an actor to the conflict?	The UNGPs state that "where business enterprises identify that they have caused or contributed to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes." (UNGP 22)
Contribute	The company's activities, when combined with those of other actors, cause harm. Contribution can be of two types: Where a tech company "**facilitates or enables**" a user to cause an adverse impact, where a company's actions add to the conditions that **make it possible** for use of a product by a third party to cause a harm. Where the company "**incentivizes or motivates**" a user to cause an adverse impact, where a company's actions **make it more likely** that a product or service will be used in ways that cause harm. In CAHRA, extend this analysis to understand facilitating, enabling, incentivizing, and motivating use and misuse of products and services to worsen conflict drivers, exacerbate grievances, or contribute to violence or instability.	Social media company amplifying hate speech by conflict actors, targeting vulnerable groups. An app store hosting an app that gamifies the humiliation of a vulnerable group. A web browsing hosting service that approves and displays ads inciting violence/hate against a vulnerable group. **Ask:** Have any market-specific changes to our design, development, and release made it easier for conflict actors to misuse our products? Have sales and promotions activities incentivized weaponization of our products? Have our business models made it easier for one conflict actor to access and misuse our data to cause harm or worsen the conflict?	
Linkage	The company has not caused or contributed to an adverse human rights impact, but there is nevertheless a link between its operations, products, or services and that impact. In CAHRA, linkage is critically important. A company's linkage to conflict could quickly **evolve into contribution** based on a lack of action or attempts to use leverage or address human rights risks in a non-conflict sensitive way.	A company's AI technology is used by a third party (with or without the company's knowledge) as a component of a new product that is then sold to a government that uses it to discriminate against certain groups while determining criminal sentences. **Ask:** Which conflict actors, or their business relationships, are using or likely to use our products to cause harm?	The UNGPs state that in this situation "the responsibility to respect human rights does not require that the enterprise itself provide remediation, though it may take a role in doing so." (UNGP 22, Commentary)

The B-tech paper observes that a tech company's involvement with an impact may shift over time "depending on its own actions, omissions and evolving standards of good practice." An end-use to which the company is directly linked could evolve into an end-use that contributes to an adverse human rights impact, if the company fails to take measures to prevent or address the impact.[26] In a conflict situation, this evolution could happen very quickly, especially if the technology has the tendency to "amplify" harmful impacts (e.g., spread of state-sponsored disinformation on a social media platform). Proactively and frequently assessing impacts, can help companies identify harms attributable to them before extensive damage is caused.

5.6. Assess leverage

Leverage—seeking to influence behaviors and practices of others who might be causing harm vis-à-vis a company's products, services, or software—is one of the key ways that companies can prevent or address the risk of adverse conflict or human rights impacts. Even when a company has taken all measures at the product design, development, deployment, and sales processes to prevent and address possible harms, inevitably, an end-user will use or misuse a product to cause harm, foment violent conflict, or gain an upper hand in a conflict. In these cases, companies need to be prepared to use any leverage they have or can establish—together or with others—to stop that end-user from causing such harm.[27]

Leverage may also be different in CAHRA, especially with respect to partner relationships and influence with governments. Some leverage may be stronger, and other points of leverage may be curtailed or could give rise to perceptions of bias.

Consider:

- *Updating software licensing or features to cut off or restrict misuse, relocating staff, or decommissioning infrastructure.*
- *Creating leverage through third parties with significant influence, such as the UN, investigative groups, humanitarian organizations, home governments, friendly states, regional bodies, other local and international companies, etc.*
- *Using third parties, such as international human rights organizations, to advocate around sensitive issues and raise awareness about relevant topics.*
- *Participating in multi-stakeholder organizations and industry-level collaborations such as GNI can help provide a venue for sharing sensitive information with trusted colleagues when you are restricted from speaking publicly.*

[26] UN OHCHR (2020). "Access to remedy and the technology sector: basic concepts and principles: A B-Tech Foundational Paper."
[27] UN OHCHR (2020). "Key Characteristics of Business Respect for Human Rights."

6 Address Impacts

6.1. Integrate conflict sensitivity for mitigations

Actions to address conflict impacts and human rights impacts in CAHRA also need to be evaluated through a conflict sensitivity lens. Mitigations can have further impacts on the conflict, for example:

- *Utilizing leverage in the international community against the conflict or particular bad actors can put employees or local staff at risk.*
- *Adjusting content moderation policies to remove violent extremist and terrorist content may prevent evidence collection for future accountability efforts or suppress freedom of expression.*
- *Adjusting algorithms to reduce the proliferation of certain content or making content-neutral adjustments can limit the opportunity for human rights defenders and local communities to share critical information and develop and share their own narrative of the conflict.*
- *Limiting access to products, services, and platforms can open the way for bad actors to use other products and services from unregulated or less scrupulous companies.*
- *Using Trust & Safety or Customer Services teams to engage with end-users about violence-promoting or hate speech in the language of a dominant ethnicity, leaving vulnerable minorities exposed.*
- *Using a software or features update that does not take into consideration conflict actors using less advanced versions of a product, service, or software.*

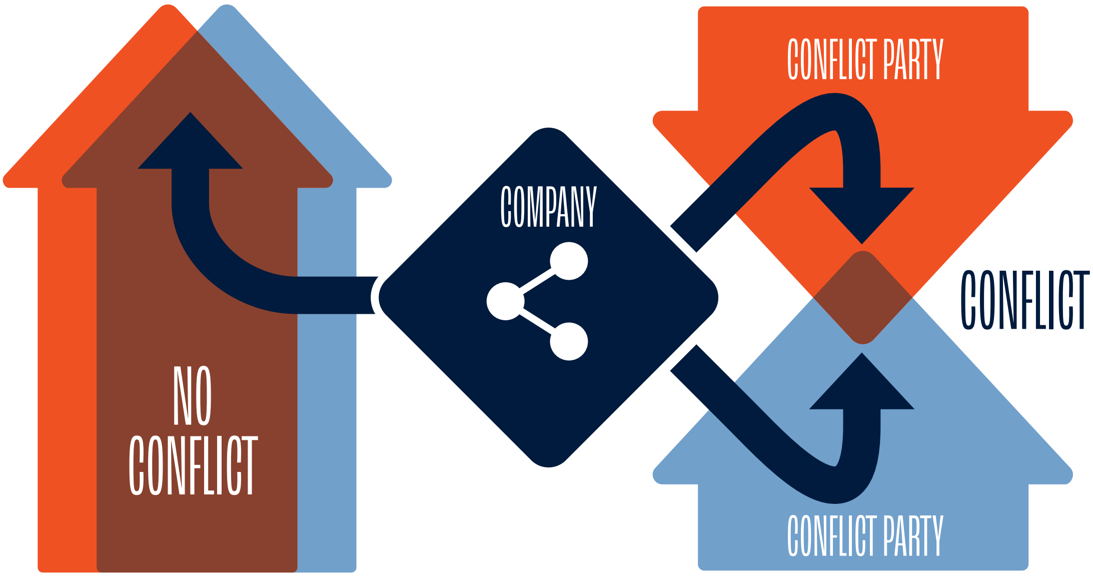
6.2. Ensure that mitigations are proportionate to the risk of harm

Tailor standard responses and mitigations to the conflict context.

Mitigations should be proportionate to the risk of harm. In CAHRA, those risks are higher, and so mitigations should be adjusted accordingly.This will likely require creating a rapid-action channel across different teams to enable changes to platforms, service updates, and communications with local staff.

Sometimes, mitigating against a conflict impact can in turn adversely impact human rights. In this case, the rights, impacts, and mitigations will have to be balanced. Sometimes, trade-offs will be necessary.

Practice tip: *Create an escalation plan and identify relevant roles, responsibilities, and internal consultations as part of the formal eHRDD policy in advance so that thresholds are mapped out and responsibilities and owners communicated in advance. This may need to be adjusted depending on the context and how the situation evolves, but pre-planning here is essential.*



For example:

- *Ethnic discrimination may not be a highly salient human rights issue in most settings, but in a conflict setting with ethnic divisions, this may become a more salient factor that needs to be addressed and can influence a company's perceived neutrality or the safety and security of employees.*
- *Reducing visibility of all reshared posts in an attempt to reduce virality of harmful content might be proportionate in some cases when the risk of severe widespread harm is high, and disproportionate in others.*
- *Internet shutdowns may be a moderately salient human rights concern, and in normal contexts, may be readily remediable. However, in a conflict situation, internet shutdowns can be weaponized to create widespread and irremediable situations of harm, including loss of life and severe injury, to vulnerable communities.*
- *Freedom of expression may be a salient human rights concern, but in a conflict situation, social media platforms can be weaponized to foment division and violence. Curtailing certain aspects of freedom of expression may be required to address impacts on the conflict itself, and irremediable human rights harms that could result.*
- *Product blacklisting could unintentionally legitimize or delegitimize conflict actors.*

Companies should take steps to avoid mitigations that will in turn cause other adverse conflict impacts. Assessing conflict impacts in addition to human rights impacts should be proportionate to the scope and scale of impact and potential leverage and mitigations.

Practice tip: *Consult with and draw on the experience of local stakeholders and rightsholders, international human rights community, peacebuilding community, and humanitarian community for experience in dealing with situations of competing priorities and human rights in CAHRA.*

6.3. Track the effectiveness of mitigation measures

In tracking the effectiveness of mitigation measures, refer to the conflict mapping and conflict sensitivity analysis. Assess any changes in the situation and how they may be related to any mitigation measures taken. Focus on whether the company's actions—taken alone or with others—have reduced risks to the adverse conflict or human rights impacts they are intended to address.

6.4. Devise a plan and strategy for when to roll back mitigations

This should be tied to the ongoing risk tiering and evaluation of conflict contexts. Conflict is often cyclical and not easily resolved. In this context, mitigations should be continuously evaluated and adjusted to fit the context. Consider when the company is capable of handling what happens in the normal course of business, and when the risk of conflict impacts and adverse human rights impacts can be addressed through standard HRDD processes.

6.5. Build mitigations into existing and planned cross-organizational outputs

Link long-term mitigation efforts to programs that reduce drivers of conflict such as bribery and anti-corruption (through the compliance and legal team) and through digital literacy programs designed to educate citizens about hate speech and misinformation (through research and policy teams) or by revising content moderation practices so they can identify dangerous patterns and narratives (through trust and safety teams).

Practice tip: *Create an escalation plan and identify relevant roles, responsibilities, and internal consultations as part of the formal eHRDD policy in advance so that thresholds are mapped out and responsibilities and owners communicated in advance. This may need to be adjusted depending on the context and how the situation evolves, but pre-planning here is essential.*

6.6. Consider responsible exit

There may be situations where a company lacks leverage to prevent or address the risk of adverse conflict or human rights impacts. In those situations, the company may want to consider ending a certain business relationship or exiting from a CAHRA. This will likely be a complex and difficult decision and will require trade-offs and balancing impacts on the conflict and human rights. Consider issues such as:

- *What are the relevant legal constraints? Are there sanctions that prohibit operations? Can the company comply with all applicable laws simultaneously (e.g., local national security provisions vs. European privacy laws)?*
- *Can a company do more to address risks by staying? Can a company address these risks by reducing the scope of products, services, or customers served? Who are competitors in this space, and would our exit leave a gap for an unscrupulous company to enter?*
- *Do vulnerable users have a critical need for the company's products and services? How would an exit impact those users? Would they be more vulnerable to the conflict, or to human rights abuse?*
- *Would exiting exacerbate the weaponization or misuse of other relevant technology products and services?*
- *What is the regulatory landscape? What is the legal risk to the company or its employees if human rights due diligence becomes legally impermissible in a CAHRA?*

Practice tip: *Consider what a "responsible exit" would require or context-specific issues to be prepared to address as part of an HRIA at the time of market entry.*

6.7. Provide operational level grievance mechanisms

In high-risk markets, there is usually weak rule of law and a non- or low-functioning judiciary. This raises the importance of having a mechanism to support remedy for victims of human rights abuses. B-Tech provides useful guidance on enabling access to remedy. When a company has caused or contributed to an adverse impact, they have a responsibility to remediate the harm.

Operational level grievance mechanisms (OGMs) allow affected stakeholders to raise concerns about any adverse impacts they have suffered due to company actions or omissions. In a conflict context, they can act as an "early warning signal" by alerting a company to potential risks that could snowball into severe adverse impacts.

These mechanisms can take varying forms, depending on the type of technology product, and could be provided at the industry level rather than at the company level. However, it is important that they be impartial and address all human rights risk, rather than just a narrow set of digital rights.

When dealing with large-scale or gross human rights abuses (e.g., a genocide) in a conflict context, the gravity and complexity of the violations can reduce the effectiveness of OGMs.[28] In such cases, it is better for the company to support those processes.

Practice tip: *The OHCHR B-tech Project provides detailed guidance on designing effective OGMs for a range of technologies, distinguishing between grievances that need a speedy response (e.g., where a journalist is being harassed and threatened with violence online) vs. those that require more review and appeals (e.g., content that indirectly praises the actions of a terrorist group) as well as between grievances that need personalized responses (e.g., where a writer's account has been suspended at the request of a government) vs. grievances that can be dealt with at scale (e.g., alerting people if they have been exposed to false information about an election in their country).*

When providing these grievance mechanisms in CAHRA, the following additional considerations should be kept in mind:

- *Account for the fact that data and reporting behaviors and information received may be influenced by which side of the conflict the individual is on.*
- *Take extra care to ensure the accessibility, safety, and security of grievance mechanisms—including to nonusers or users without registered accounts. This includes guaranteeing confidentiality or anonymity, where appropriate, as well as ensuring that data collected through the grievance mechanism is stored safely and securely (e.g., end-to-end encrypted and password protected).*
- *Ensure that grievance mechanisms are set up to transfer reports to the appropriate body internally and externally. Internal teams should be equipped and trained to triage, escalate, and follow up rapidly and appropriately, given the shorter time frame of serious events in high-risk markets.*
- *Account for limitations of automated or algorithmic decision-making systems, such as in understanding complex social issues and people's personal experiences and be transparent about the extent to which the company relies on them within grievance processes.*
- *Use OGMs to support transitional justice and post-conflict reconciliation efforts, such as evidence collection and preservation, or participate directly in them if the company had a role in the conflict.*

[28] International Commission of Jurists, (Nov. 2019). "Effective Operational-level Grievance Mechanisms."

7 Communicate Progress

UNGP guidance to communicate publicly about HRDD processes so that external stakeholders can meaningfully evaluate company efforts holds true in CAHRA. However, exercise caution when deciding how, when, and what to publish about eHRDD processes in CAHRA, to avoid:

- *Further influencing the conflict,*
- *Perceptions of bias or "taking a side,"*
- *Putting employees, contractors, or business partners at risk,*
- *Putting external stakeholders and those consulted in the eHRDD process at risk, or*
- *Communicating technological solutions that would allow end-users to avoid or exploit prevention and mitigation steps.*

Consider strategies such as:

- *Limiting communication to affected stakeholders (or their legitimate representatives), who are most likely to be impacted by certain end-uses of the technology. Smaller companies too could limit communications to those most likely to be impacted.*
- *Establishing regular communications or updates about related issues when a situation is steady, or low intensity, so that updates are perceived as routine. Sensitive topics can be alluded to in those routine communications with less risk.*
- *Using third parties or trusted industry groups to communicate certain topics that are too sensitive for corporate communications.*

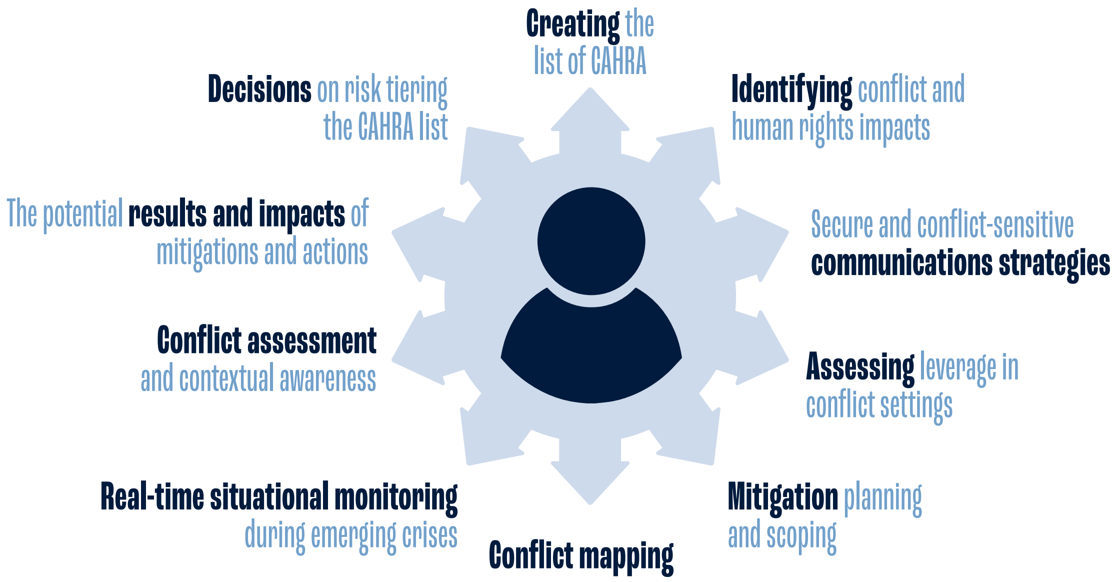
These considerations also apply to backward-looking assessments of a company's role in a specific conflict during a specific time. Conflicts are cyclical, and some risks may arise again in the future even if a conflict appears to have been resolved for the time being.

8 Cross-Cutting Issue: Stakeholder Engagement

Stakeholder engagement is an essential part of eH-RDD. Diverse stakeholder input is needed to help build nearly every stage of this process.

Engagement should be equitable and provide meaningful opportunities for stakeholders to raise issues and see the impact of their recommendations. It is important for stakeholders to understand what is done with the information they provide and what is or is not useful to companies.

Building long-term relationships with civil society actors can position companies to be able to quickly engage in a crisis, have a connection to on-the-ground representatives, and to do important translation work and discussions about how companies operate before timing becomes shortened and stakes rise.


Creating the list of CAHRA
Identifying conflict and human rights impacts
Secure and conflict-sensitive **communications strategies**
Assessing leverage in conflict settings
Mitigation planning and scoping
Conflict mapping
Real-time situational monitoring during emerging crises
Conflict assessment and contextual awareness
The potential **results and impacts** of mitigations and actions
Decisions on risk tiering the CAHRA list

8.1. Build a specific eHRDD engagement strategy

Build a specific eHRDD engagement strategy. It should establish a process and objectives for engagement and roles and responsibilities. Focus on how to protect the security and safety of those you engage with. This overall plan can then be further tailored and updated as needed for each CAHRA.

Use participatory methods that actively engage community members in the assessment, such as focus groups or multi-stakeholder meetings. Provide independent interpretation and the opportunity for participants to express their views in their local languages.

Consider the perceived legitimacy of the engagement, and take steps to ensure that those tasked with engagement are familiar with the local setting and that they generate trust and confidence among affected communities and local stakeholders.

8.2. Create context-appropriate engagement processes

Use the conflict sensitivity lens (discussed above) to plan and execute engagement. Engagement plans may be different for "high risk" and "medium risk" areas with issues that can be addressed in advance, and situations that have evolved into crisis or high-intensity conflict. An example of differences could include:

High Risk / High Intensity	Medium Risk	Stable/Low Intensity
▪ Stakeholders have limited time or capacity to meet. ▪ Trust and existing relationships will be key. ▪ Prioritize engagement on crisis-related issues and any urgent needs. ▪ Security risks will be high. ▪ Consider using third parties or creative means to connect if security requires.	▪ Opportunity to deepen trusted relationships. ▪ Consider engagement methods with international organizations and other trusted third parties working in the context. ▪ Prioritize engagement on understanding the conflict and the company's role in it, as well as identifying conflict and human rights impacts. ▪ Security risks may be high.	▪ Opportunity to build new relationships with broad representatives of vulnerable groups and rightsholders. ▪ Consider in-person and in-country engagements. ▪ Consider using community-based engagement methods. ▪ Engagement topics can be broad and cover issues such as product use, media mapping, etc.

Depending on the context, engagement can be both **long term** and **short term**. Long-term engagements are better at surfacing key impacts because stakeholders have had more time to better understand the technology and its uses. They also provide opportunities to gather proactive, rather than reactive advice and take appropriate measures. Short-term engagements may be effective for urgent crisis response situations with concrete objectives.

8.3. Plan ahead

Get an early start. Having established and trusted relationships in place during times of relative peace is invaluable when crisis emerges. Building long-term relationships with civil-society actors can position companies to quickly engage in a crisis, have a connection to on-the-ground representatives, and to do important translation work and discussions about how companies operate before timing becomes shortened and stakes rise.

Stakeholder engagement should not wait until a conflict intensifies. During conflict and crisis situations, local stakeholders will be under immense pressure, strain, or risk, and may not be readily available for engagement opportunities.

However, should any stakeholders reach out from intense conflict areas or conflict-affected settings, engagement with them should be prioritized.

8.4. Garner resources

Secure additional resourcing early, to ensure broader, regular, and holistic engagement, including with external experts who may need to become part of crisis response teams. This should be assessed based on the level, frequency, and type of engagement needed.

Practice tip: *Consider providing financial support. Many stakeholders are CSOs which depend on external funding to maintain their ability to engage with companies. This raises the question of whether their independence or credibility could be compromised when they receive funds from companies they engage with. This question is relevant for both transactional funding (companies reimbursing stakeholders for a specific engagement) and institutional funding (companies funding ongoing multi-stakeholder initiatives). For transactional funding, companies typically address these concerns by reimbursing expenses and/or making a nominal charitable donation to an organization of the stakeholder's choice. For institutional funding, key principles include transparency about where funds are coming from and relying on diverse sources of funds.*

8.5. Take a cross-functional approach

Consider linking eHRDD stakeholder engagement to efforts by teams such as:

Anti-corruption or bribery programs	Identify links between corruption, conflict, and business activities and demonstrate the company's commitment to anti-corruption.
Trust & Safety departments	Identify potential stakeholders and sensitive topics or issues that are coming through these channels; can be an opportunity to engage with users on digital literacy or educational campaigns on hate speech or misinformation.
Market teams	Engage with partners, suppliers, business and trade associations, or government departments.
Public Affairs	Work with diplomatic partners, home state, and other third-party states and international organizations.
Other verticals	Day-to-day decisions about human rights issues, such as removing user-generated content, responding to law enforcement demands, or designing product functionality and permissions happens across different verticals within the company. Employees who make decisions about these things can benefit from hearing directly from the most vulnerable and ensuring decisions are more rights-respecting.

8.6. Ensure holistic, sustained, and meaningful engagement with diverse rightsholders

The results of the conflict-assessment and identification of vulnerable groups should inform the engagement strategy. Rightsholders impacted by the conflict may be different from those engaged with from a standard human rights assessment. They may extend beyond the typical user or customer profile.

In a conflict context, it is likely that most engagement will be with representatives of rightsholders due to security concerns.

Consider engaging with:

- *Rural communities*
- *Diverse ethnic and identity groups*
- *Diaspora groups (in addition to, not in lieu of, local groups)*
- *Diverse political groups*
- *Marginalized groups*
- *Women and girls*

8.7. Engage with business groups, governments, and conflict actors

Stakeholder engagement also extends to peer businesses, trade groups, home governments, host governments, and diplomatic actors. Any engagement with governments or regional bodies must be undertaken with an understanding of their role in the conflict, regional and geo-politics, and potential biases or perceptions of bias if the company is seen to be biased toward the government. Safety of local staff should be a key priority when deciding on engagement approaches.

Home governments have a duty to protect human rights under Principle 7 of the UNGPs and to support companies based in their jurisdiction in identifying and responding to heightened human rights risks. Engagement with them should include asking for diplomatic and intelligence support to assess and address conflict risks.

Host governments and regional bodies provide an opportunity to promote human rights through direct and indirect advocacy. Direct advocacy can include pushing for regulatory reform, rule of law, and human rights protections by articulating a shared interest in economic development and stability. This could include taking a position in favor of rule of law generally or advocating for market-specific regulatory changes. Advocacy may be either public or discreet, and it may be undertaken collectively or alone, with joint advocacy typically providing greater protection from targeted consequences.

Armed groups and conflict actors should also be identified, and companies should proactively establish a strategy for engaging these stakeholders safely and impartially. When engaging with different stakeholders, seek to maintain impartiality and independence from government-led or armed-group-led efforts.

Practice tip: *Using third parties, including home state diplomatic representatives, business groups, local trade entities, humanitarian organizations, or trusted multi-stakeholder groups such as GNI, etc., can be useful here.*

8.8. Anticipate and plan for barriers to access

Engagement strategies should anticipate and plan for unique aspects of conflict settings, including barriers to participation such as:

- *Barriers that might be related to the conflict situation or emerging barriers as the conflict evolves.*
- *Remote location and challenges to access such as seasonal weather (e.g., rainy season) impacting travel.*
- *Alternative language, digital literacy, and other access capacities.*
- *Systemic or cultural biases may impede access to some groups, such as women or other marginalized groups.*
- *Competing priorities and limited ability, time, or capacity to engage when in a war zone or active crisis.*
- *Risks to stakeholders of engaging directly with companies.*

Engagement should be equitable and horizontal—not "top down," but mutually beneficial—and provide meaningful opportunities for stakeholders to raise issues and see the impact of their recommendations.

8.9. Ensure balance and address potential bias

It may be difficult or impossible to find neutral parties in conflict contexts. Here, understanding the conflict can help you understand potential bias and how to ensure you are speaking to diverse stakeholders who represent all sides of a conflict.

Assess how to find the best source of truth, how to counteract the effect of polarized beliefs, where to find the most accurate sources of information, and where conflict actors themselves are trying to influence narratives and information shared with companies and external groups. This should be informed by the conflict mapping and conflict sensitivity assessments discussed above. Consider hiring experienced consultants and/or anthropologists who are familiar with international social assessment standards and have knowledge of local social and cultural dynamics.

8.10. Assess and plan for security concerns

Safeguard the safety and security of stakeholders during engagement. This requires an ongoing analysis. Security measures should be sustained in future engagements related to that situation, including transparency and communications efforts, public-facing events, workshops, panel discussions, or conferences whether held locally or internationally.

Risks for stakeholders during engagement could include physical security risks, cybersecurity risks, sexual and gender-based violence risks, and political co-option. Alternative methods should be employed to ensure the input of rightsholders who cannot participate in stakeholder engagement due to security risks. These methods include consulting independent experts, working through NGOs or embassies, and encrypted email and phone communication.

Example: *If there are events or group engagements planned that might bring together diverse conflict actors or representatives from different sides of the conflict, and ensure that potentially vulnerable individuals are informed of this, and their security preferences acted upon.*

Example: *Sometimes, simply communicating a fact about a situation could put stakeholders or employees at risk if the company were not, according to conflict actors, aware of that fact. Certain information disclosure may endanger vulnerable individuals or fuel conflict, and so all communications in high-risk or conflict-affected areas should be undertaken with care to limit any associated harm.*

8.11. Be creative and flexible, and use third parties

Sometimes contextual challenges (see above on mapping conflict actors, barriers to access, and security) require creative approaches and alternative methods of engagement.

Consider collaborating with credible third parties to design engagement strategies and enable alternative channels of information like operational level grievance mechanisms.

Practice tip: *External stakeholders may need to be supported to learn about technical issues and processes that are relevant to a company's human rights commitments. Establish ways of sharing this information while considering legitimate concerns about IP confidentiality and commercial sensitivity.*[29]

8.12. Consider different ways to engage

Engagement can take many forms, including:

- *Interviews*
- *Analysis workshops*
- *Focus group discussions*
- *Surveys*
- *Trusted partner | flagger programs*
- *Special reporting | escalation channels*

Practice tip: *COVID-19 and other travel restrictions related to crisis situations emphasize the need to start engagement early, and to build it into an ongoing eHRDD plan. It may require the use of trusted partners in country who can help facilitate connections, interviews, focus groups, or surveys with local rightsholders and communities that do not have access to digital engagement tools (e.g., video or voice calls).*

[29] UN OHCHR (2020). "Key Characteristics of Business Respect for Human Rights: B-Tech Foundational Paper."

9 Cross-Cutting Issue: Leverage Industry-led and Multi-stakeholder Collaboration

Industry-led collaboration can help build efficiencies and broaden understanding of risks and potential mitigations. It can help companies pool resources to address high-risk situations where conflict appears to be intensifying, allowing companies with no formal market presence or very low user numbers to broaden their understanding of the situation and work within existing resource constraints to plan a response and mitigations.

Collaboration can be valuable across industry segments as well. Companies with significant infrastructure and staff in CAHRAs such as telecommunications companies have a shared interest with other tech companies with significant "presence" in a country but no staff or infrastructure. Companies would have a shared interest in and knowledge of the conflict context and can bring different and valuable information to collaborative efforts.

Industry collaboration in a pre-competitive environment could include collective efforts on:

- **Research, data collection, and analysis:** *Streamlining and customizing data sets for the tech industry or sector, in particular relational data comparing countries and situations; sharing information and analysis about the evolving context and conducting ecosystem or conflict mapping.*
- **Risk assessment:** *Establishing guidelines and criteria for thresholds, risk categories, and responses; conducting sector-wide joint conflict assessments and conflict and human rights impact assessments of regions or common high-risk business partners (e.g., those with government or military affiliations).*
- **Capacity-building:** *To address common challenges or where infrastructure is shared (e.g., use of telecom towers leased from the same government).*
- **Exercise leverage:** *When one company's leverage alone is insufficient to prevent or address human rights abuses (e.g., industry-wide sales bans or moratoriums of specific products, customers, or markets; building leverage with business partners who are government entities; consensus on high-risk and no-go sales). This can particularly include collective action on anti-corruption efforts, which are often front-line defenses for major conflict drivers like the plundering of resources and government impunity for crimes against its citizens.*
- **Regulatory reform:** *Advocate collectively for regulatory reforms, rule of law, and respect for human rights.*
- **In-country stakeholder engagement:** *The information gleaned from the above efforts can be used to engage with internal stakeholders and position them around action and prevention.*

Most pan-industry collaborations are still predominantly Western in their membership, thus limiting the variety of perspectives from non-Western contexts, which are crucial for understanding conflict. These collaborations (e.g., GNI, DTSP, GIFCT, BSR's Human Rights Working Group and Tech Against Terrorism) should continue to increase non-Western company and civil society participation and ensure a high degree of connectedness with real local challenges.

To be successful, collaborative organizations must ensure a constant flow of informed civil society perspectives from high-risk locations through more direct engagement with rights holders on the ground. To do this, they could consider the creation of local chapters that support local conversations.

They should also provide pathways for engagement with governments, including both home and host governments.

Toolbox

Additional reading

- BSR (2022). "Rapid Human Rights Due Diligence During Political and Armed Conflict: A Business Response to Ukraine."
- BSR (2022). "Human Rights Impact Assessment on Meta's Expansion of End-to-End Encryption."
- BSR (2022). "Applying the UNGPs to Technology: Our Point of View."
- BSR (2021). "Access to Remedy."
- BSR, (2021). "Seven Questions to Help Determine When a Company Should Remedy Human Rights Harm under the UNGPs."
- BSR, (2021). "Responsible Product Use in the SaaS Sector."
- Conciliation Resources (2015). "Gender & conflict analysis toolkit for peacebuilders."
- Conflict Sensitivity Consortium (2012). "How To Guide to Conflict Sensitivity."
- DCAF and ICRC (2019). "Addressing Security and Human Rights Challenges in Complex Environments."
- Easterday, J., Ivanhoe, H., and Schirch, L. (2022). "Comparing Guidance for Tech Companies in Fragile and Conflict-Affected Situations," Toda Peace Institute Policy Brief No. 125.
- EU External Action (2014). "Factsheet: EU Conflict Early Warning System."
- Ferroggiaro, W.; Mercy Corps (2021). "Social Media, Conflict, and Peacebuilding: Issues and Challenges: Discussion Paper."
- Herbert, S.; GSDRC, University of Birmingham (2017). "Conflict Analysis: Topic Guide."
- International Alert (2008). "Red Flags: Liability risks for companies operating in high-risk zones."
- JustPeace Labs (2021). "Technology in Fragile Contexts: Engagement, Partnerships, and Positive Action."
- JustPeace Labs (2020). "Technology in Conflict: Conflict Sensitivity for the Tech Industry."
- Mercy Corps (2019). "The Weaponization of Social Media."
- Mercy Corps (2021). "Analyzing and Responding to Social Media and Conflict."
- Schirch, L., ed. (2021). "Social Media Impacts on Conflict and Democracy: The Techtonic Shift," (Routeledge).
- Shift, Oxfam and Global Compact Network Netherlands, (2016). "Doing Business with Respect for Human Rights: A Guidance Tool for Companies."
- UNDP (2017). "Conducting a Conflict and Development Analysis."
- UN office on Genocide Prevention and the Responsibility to Protect, "Early Warning."
- UN OHCHR, B-Tech Foundational Papers.
- Voluntary Principles Initiative (2022). "Voluntary Principles Initiative Conflict Analysis Tool for Companies."

UNGPs relevant for enhanced HRDD in CAHRA

Principle	What It's About	Why It Matters for eHRDD
Principle 7	Lays out duties of home states to support corporate eHRDD in CAHRA.	Tech companies often have a widespread, even global, presence, while maintaining employees and physical offices in a handful of countries. This can impact leverage.
Principle 12	Broader scope of corporate responsibility in CAHRA; respecting standards of IHL.	IHL influences how tech companies should react or respond to government requests for data or other actions.
Principle 17	Possible complicity in gross human rights abuses and legal liability.	Tech companies could be exposed to legal liability, where their products and services are used in the commission of atrocity crimes, a high risk in CAHRA.
Principle 18	States that HRIAs are necessary when there are significant shifts in local operating contexts; commentary recommends inclusive stakeholder engagement.	The highly distributed nature of technology companies means that they need to continuously monitor diverse operating contexts.
Principle 22	Establishes the requirement for remedy.	Foundational Principle of eHRDD.
Principle 23	Provides the basis for eHRDD in conflict-affected settings.	Foundational Principle of eHRDD.

Leveraging internal teams beyond the human rights team

Team	eHRDD Roles and Responsibilities
Public Policy or Public Affairs	Identify and flag certain conflict triggers in CAHRA (e.g., social, political, regulatory, economic etc.); advocate for rights-respecting regulation; build local and regional partnerships; help streamline eHRDD with other policies; assess risks and leverage.
Compliance	Integrate human rights and conflict risk into ERM frameworks and other compliance processes.
Legal	Flag legal risks that could also be human rights risks (e.g., bribery and corruption); manage law enforcement demands for user data / content restrictions / shutdowns / interception and flag those which don't meet human rights standards. Assess process under DSA and other mandatory HRDD regulations.
Trust and Safety	Flag patterns of harmful content (e.g., hate speech and misleading narratives) and misuse of product functionalities (e.g., use of duplicate accounts to amplify hate speech) as well as traits of vulnerable groups and the ways in which they are targeted.
Security	Flag emerging threats to user security such as DDoS attacks, hacking, phishing, malware, and similar security issues perpetrated by conflict actors. Provide insight into law enforcement assistance relationships and obligations. Evaluate security-based decisions on what it could mean for staff, customers, consumers, and communities in conflict-affected areas.
Sales	Integrate a human-rights risk lens when considering sales to conflict actors (e.g., authoritarian governments, law enforcement, state-owned enterprises, etc.) or their business relationships.
Privacy	Strengthen privacy protections for vulnerable users in conflict contexts, minimizing opportunities for attacks. Flag any potential risks.
Product	Minimize vulnerabilities in the product which could be exploited by conflict actors. Flag any potential risks.
Research	Flag risks based on the interaction of products and services (in-use and planned) with different user types in conflict areas.
Crisis Management	In addition to identifying and mitigating "risks to the company," also identify risks to human rights in conflict contexts and work cross-functionally to address and prevent adverse impacts. Raise and provide insight on potential reputational issues.
Investor Relations	Understand investor concerns around human rights and share with other cross-functional teams. Highlight proactive steps taken to integrate respect for human rights across functions.
Human Resources	Strengthen employee safety measures (both physical and mental) in conflict contexts. Flag any potential risks that could be exacerbated by the conflict situation (e.g., discriminatory behavior or barriers to working).
Procurement	Flag any human rights concerns relating to suppliers such as modern slavery, child trafficking, etc. as these can be indicators of conflict.
Marketing	Ensure that marketing and promotional efforts are also conflict sensitive and are not promoting products and services in a CAHRA that can drive conflict.
Communications	Integrate a conflict-sensitive lens in communications strategies in CAHRA and related topics, being sure to assess impact on the conflict, perceptions of bias, and security of employees, partners, and communities. Tackle potential reputlational issues.

External sources for CAHRA list

External Sources	Rationale
Indices tracking conflict and human rights contexts (e.g., ACLED, Uppsala Conflict Data Program, V-Dem, World Bank list of Fragile and Conflict-Affected States, Fragile States Index, Early Warning Project, Freedom House Global Freedom Map, HRMI, etc.)	These are quantitative country rankings or scores, typically prepared by civil society or academic organizations and updated with some frequency (e.g., yearly, bi-annually or monthly). It is important to ensure that the methodology for the classification and the donors / funders to the project are transparently shared on their website.
Conflict and human rights reports (e.g., reports and updates by RULAC, Heidelberg Conflict Barometer, International Crisis Group, Human Rights Watch, Amnesty International, AccessNow, Article 19, etc., US State Department Reports on Country Practices, as well as reports and updates by local and regional civil society organizations).	These are qualitative reports published by leading international nonprofits as well as governments. These should be supplemented with reports from local and regional civil society organizations. To prevent any bias, ensure that the organization lists its funding sources on its website.
Current events and media searches	These are integral to building awareness about day-to-day developments and the broader social, political, and economic context in the country. These can also provide information on upcoming events or political moments that can destabilize.
Other red flags (e.g., indicators that a situation is escalating and intensifying).[30]	▪ Amassing of weapons, especially arms, especially by non-state groups. ▪ Weak or absent state structures, including the imposition of emergency laws or extraordinary security measures, or the suspension of, or interference with, vital state institutions, particularly if this results in the exclusion of vulnerable or minority groups. ▪ Records of serious violations of international human rights and/or humanitarian law. ▪ Increased inflammatory rhetoric or hate speech targeting specific groups or individuals. ▪ Signs of militia or paramilitary group recruitment, public appearances or other activity. ▪ Strengthening of the state security apparatus or mobilization against specific groups. ▪ Strict control or banning of communication channels; including control of media and distortion of facts, censorship, propaganda, misinformation and lack of access to reliable objective information, lack of objective independent media (TV and radio), and closure of internet or websites. ▪ Expulsion or banning of non-governmental organizations, international organizations, media, or other relevant actors. ▪ Groups of individuals at the mercy of an authority they oppose or that perceives them as the enemy, and members of their families and communities. ▪ People are not protected from acts of violence perpetrated against them. ▪ People are unable to meet their basic needs because of a climate of fear and violence. ▪ Presence of displaced persons including those who are internally displaced.
Ongoing stakeholder engagement, including with in-country groups and experts.	Local stakeholders, rightsholders, and civil society groups are invaluable sources of information for understanding when conflict may be escalating and the impact of the company's products and services on the conflict. They can also serve as channels for learning about unanticipated issues as the context evolves.
Internet penetration and comparison to number of users	Understanding the scope of digital penetration and digital literacy can provide a fuller understanding of technology's impact on conflict dynamics, especially with respect to free products and services in areas that are not explicit company markets.

[30] Adapted from UNDP and the UN Working Group on Business and Human Rights (2022). "Heightened Human Rights Due Diligence for business in conflict-affected contexts."

Internal data on relevant markets and business activities

Internal Factors	Rationale
Number of users or scope of presence and financial recovery	This will help determine the potential scope and scale of impact on the conflict and human rights.
Location and number of local offices, employees, or suppliers	This will help indicate an “on the ground” presence and any heightened security concerns.
Reports from Trust and Safety or Health teams	Can help provide color and context about user behavior and flag increases in potential adverse impacts.
Feedback from regular meetings with internal stakeholders (security team, local risk teams, product teams, customer research teams).	Provides an overview of the context, mood, and potential risks identified by these other teams.
Other red flags	These can be indicated by an above average and persistent spike in the following: ▪ Borderline content which has the potential for inciting, or has incited,violence. ▪ Overbroad government requests for user data, content takedowns, and censorship targeting primarily those from a vulnerable group such as journalists, human rights defenders, or ethnic minorities. ▪ Law enforcement demands that do not indicate what the investigation is for, indicating a risk that “legal” requests for data could be weaponized or used for intentional human rights violations. ▪ Repeated government requests for internet shutdowns, especially targeting a particular city or state. ▪ Disinformation attacks led by state actors or those affiliated to them, as well as by powerful non-state actors, usually targeting a vulnerable group. ▪ Requests for publishing ads that can incite violence or other offline harm, often made by powerful state or non-state actors.

Salience measurement: sample tool

Issue	Scope	Scale	Remediability	Likelihood	Prioritization
X	Medium	Minor	Remediable	Highly likely	Tier 1
Y	Very large	Moderate	Possibly remediable	Unlikely	Tier 2
Z	Very small	Extreme	Not remediable	Likely	Tier 1

**The scales for each of these categories (e.g., high, medium, low) and their definitions would vary by the type of technology, end-use, and operating context*

CAHRA risk tiering: sample tool

Threat of death or injury to protesters	Impact Severity (weighted higher)	Likelihood (weighted higher)	Leverage (weighted higher)	Impact Category (weighted higher)	Timeframe	Market Share	Risk Score
Country A	Severe	Certain	Moderate	Direct	Immediate	Low	Very high
Country B	Severe	Low	Low	Cumulative	Immediate	Very high	High
Country C	Moderate	Moderate	High	Direct	Ongoing	Very high	Medium

**The scales for each of these categories (e.g., high, medium, low) and their definitions would vary by the type of technology, end-use, and operating context*

Guide to understanding the conflict

These are important topics to research to understand conflicts.[31] Several external resources can help with this, including assessments and descriptions of conflict created by RULAC and by the International Crisis Group.

- *What is the context influencing the violence or conflict?*
  - *Is there a history of conflict?*
    - When?
    - Where?
    - What were those previous conflicts about?
    - How many people have been killed and displaced?
    - Who has been targeted?
    - Were there peace processes or peace agreements? What did they agree, and how did they shape the current conflict?
  - *What methods of violence or oppression have been used?*
    - Do any of these rely on or use the company's products or services?
  - *What political, economic, social, and environmental institutions and structures have shaped the conflict (e.g., elections, reform processes, economic growth, inequality, employment, social groups and composition, demographics, the role of businesses and resource exploitation)?*
- *Who are the actors influencing the conflict?*

[31] Adapted from UNDP and the UN Working Group on Business and Human Rights (2022). "Heightened Human Rights Due Diligence for business in conflict-affected contexts."

- *Who are the main actors (e.g., the military, leaders and commanders of non-state armed groups, criminal groups, political or religious leaders, influential persons in the community, businesses)?*
- *What are their interests, concerns, goals, hopes, fears, strategies, positions, ideologies, preferences, worldviews, expectations, and motivations (e.g., autonomy, inequality between groups ["horizontal inequality"], political power, ethno-nationalism, reparations)?*
- *What power do they have? How do they exert power? What resources or support do they have? Are they vulnerable? (For example, do they have local legitimacy through provision of security, power over corrupt justice institutions, weapons, and capacity to damage infrastructure?)*
- *What are their incentives and disincentives for conflict and peace (e.g., benefitting or losing from the war economy, prestige, retribution for historic grievances)?*
- *What capacities do they have to affect the context?*
- *Who could be considered spoilers (i.e., individuals and organizations that believe peace threatens their power, worldview and interests, and who seek to undermine attempts to achieve it)?*
- *What divides people? Who exercises leadership and how? (For example, are they economic beneficiaries of conflict, criminal groups, opposition leaders?)*
- *What are the relationships between actors? What are the trends? What is the strategic balance between actors (who is "winning")? (For example, are the relationships conflictual, cooperative, or business-based?)*

- *What are the causes of the conflict?*

  - *What are the structural causes of the conflict (e.g., unequal land distribution, political exclusion, poor governance, impunity, lack of state authority)?*
  - *What are the proximate causes of the conflict (e.g., arms proliferation, illicit criminal networks, emergence of non-state armed actors, overspill of conflict from a neighboring country, natural resource discoveries)?*

- *What are the current dynamics | trends of the conflict?*

  - *What are the current trends of the conflict? What recent changes in behavior have there been? (For example, have acts of conflict increased but the number of deaths decreased? Has political violence intensified around local elections? Has defense spending increased? Have paramilitaries started running in local elections?)*
  - *Which factors influencing the conflict's profile, actors, and causes reinforce or undermine each other? Which factors balance or mitigate others? (For example, horizontal economic and political inequalities can increase the risk of conflict; uncertainty about succession of the president strengthens party factionalism; cash for disarmament, demobilization, and reintegration fuels the proliferation of small arms.)*
  - *What are, or could be, the triggers of the conflict (e.g., elections, economic and environmental shocks, an economic crash, an assassination, a coup d'état, increased food prices, a corruption scandal)?*
  - *What scenarios can be developed? (For example, in a best-case scenario, a peace agreement is signed quickly and the conflict parties implement a ceasefire; in a worst-case scenario, local politicians mobilize along ethnic lines in the run-up to elections and political violence and riots increase where groups meet.)*

- *Open source and (social)-media monitoring: These tools should be used or adapted in conflict-affected contexts to gather open-source intelligence such as conflict-related news, public perceptions of the company, and narratives of the conflict parties and other stakeholders to support or conduct the conflict analysis.*

  - *What positions do parties to a conflict (governments, opposition parties, civil society, armed groups, diasporas, etc.) convey through online communication to promote their own narratives and counter-narratives on issues relating to the conflict?*
  - *Are the competing narratives on the causes of the conflict used to incite hatred, violence, and fear, and to disseminate misinformation and disinformation?*

BSR

BSR™ is a sustainable business network and consultancy focused on creating a world in which all people can thrive on a healthy planet. With offices in Asia, Europe, and North America, BSR™ provides its 300+ member companies with insight, advice, and collaborative initiatives to help them see a changing world more clearly, create long-term value, and scale impact.

www.bsr.org

JUSTPEACE Labs

JustPeace Labs supports ethical and responsible approaches to technology deployed in high-risk settings. Our work advances peace and human rights protections around the world through advocacy, awareness raising, and research on effectively shaping corporate policy on conflict-sensitive tech design and development. We provide strategic research, policy guidance, and analysis to diverse stakeholders who use or provide technology in high risk settings.

www.justpeacelabs.org