






TrustWorks Global Conflict Risk Typology

CATEGORY	DESCRIPTION	EXAMPLES OF EXPOSED INDUSTRIES	EXAMPLES OF CONFLICT RISKS
1 Sourcing  Minerals and metals  Agricultural products	<ul style="list-style-type: none"> Sourcing activities might take a range of forms and relate to a broad range of goods. Sourcing might thereby generate different risks for different companies. Sourcing may link companies with any abuses, conflict impacts, or violations of IHL committed by their suppliers or by producers of the good that the company utilizes in its business processes. Issues that are of material concern may also differ significantly by industry. 	<p>Cosmetics; construction semiconductors and computers; jewellery; transportation systems automotive; data centres; textiles</p> <p>Cosmetics; food; nutrition; health care; beverages; textiles; farming</p>	<ul style="list-style-type: none"> The production of minerals, metals, and stones can be closely tied to or controlled by illegal armed groups or to financing conflict in other ways. In some instances there may be a risk that sourcing these raw materials links companies to these groups and contributes to financing conflict. Commercial agriculture across a range of sectors may be predicated on contested, dubious, or forcible land acquisition. Agriculture may tie companies to actors that have engaged in land acquisition processes that underpin/are underpinned by violent conflict.
	<p>Users and clients may use the company's products or services for purposes related to conflict or abuses of human rights, thus tying the company indirectly to the abuses.</p>	<p>Communication technology; security systems; semiconductors and computer; internet infrastructure</p>	<ul style="list-style-type: none"> Exposure to risk occurs through the activities of the users and the clients of products/services provided by companies. Companies that furnish dual-use technology, hardware, and infrastructure with legitimate purpose can be used for purposes that advance conflict or are criminal in nature.
3 Privacy and data protection 	<p>Risks arise through the provision of hardware, software, and services to actors, such as abusive states, that might use them for conflict-related means or abuses of human rights.</p>	<p>Data storage; communications technology; fintech</p>	<ul style="list-style-type: none"> Risk may be elevated in cases in which governments that are contested or widely perceived to be illegitimate pressure companies to turn over the personal information or communications of dissidents/ their families. Governments or armed groups may utilize IT infrastructure or capabilities to further conflict objectives.
4 Financial transactions 	<p>Risks and impacts arise through providing financial services, knowingly or unknowingly, to conflict actors or criminal organizations, allowing them to finance dubious activities or to finance or profit from - dubious activities.</p>	<p>Online banking; online payment providers; fintech</p>	<ul style="list-style-type: none"> Conflict actors and criminal organizations may use banking and payments systems to launder money, move stolen assets, or finance conflict directly through the purchase of munitions, payments to armed combatants, or similar.
5 On-the-ground operational impacts 	<p>Impacts on conflict arise from a company's presence and activities in conflict-affected regions. This category of conflict risk is particularly (though not exclusively) salient to industries that are land-intensive.</p>	<p>Extractive; renewable energy; agriculture; construction</p>	<ul style="list-style-type: none"> Benefits distribution, which refers to jobs, contracts, and development or CSR projects, and intangible benefits e.g. prestige of being an interlocutor of the company, that stakeholders perceive to be unfair; Behaviour, which includes formal positions taken by the company and the behaviour of company personnel, their suppliers and contractors, which stakeholders perceive to be disrespectful or uncaring; A narrow or legalistic approach to side-effects, e.g. events that occur as a consequence of the presence and activities of the company; and A lack of transparency, particularly about issues that affect stakeholders.