

Shift



**Weapons,
Dual Use tech and
Financial Institutions**

Weapons, Dual Use tech and Financial Institutions

By Ashleigh Owens

Acknowledgements

This briefing was written by Ashleigh Owens, who leads Shift's work with financial institutions. This briefing draws (in “Approach 5”) on previous research on export control regimes prepared for Shift by Theo Jaekel. Shift thanks Dr Branka Marijan of Project Ploughshares for valuable comments.

Today's financial institutions are operating in a global geopolitical context marked by multiplying conflicts, shifting political alignments and a decline in respect for international law. Moreover, technological developments are redefining the methods of conflict.

In this environment, financial institutions face growing pressure from governments to navigate defense-related clients and transactions in ways that **support evolving security priorities**. They also have **strong commercial incentives** to participate in a rapidly expanding sector.

At the same time, institutions remain bound by long-standing commitments to responsible investment and lending practices. And we continue to see a large body of data showing that conflict - including the impacts on people's human rights arising from conflict - creates business and investment risks for financial institutions. Importantly, in a turbulent geopolitical context, institutions that **adapt their policies and decisions in response to one particular conflict can quickly find themselves applying those policies to very different conflict situations**, where alliances, actors and the justifications for the use of force are far less settled.

Against this dynamic backdrop, financial institutions face a practical question: **how should human rights due diligence (HRDD) be approached in relation to companies developing, producing, brokering, selling or exporting weapons and dual-use technologies?**

Shift has engaged over many years with investors and lenders to support them in understanding and addressing human rights risks across their portfolios. Conflict-affected and high risk areas have been a regular feature of this work, and increasingly so in the last 4 years, since the beginning of the war with Ukraine. Through this work, we have observed a number of recurring challenges that investors and lenders face in trying to navigate complex decisions amidst often competing incentives. **While there are, perhaps fittingly, no 'silver bullet' solutions when it comes to defense-related risks**, we have found a number of approaches that can help financial institutions navigate this complex and rapidly evolving terrain. In other words, there are anchors of clarity that remain stable even in dynamic risk environments.

This briefing is divided into three parts.

Part A

sets out particular challenges faced by practitioners within financial institutions who are tasked with managing human rights risks when it comes to defense-related lending and investing.

Part B

sets out some key 'anchors' in international humanitarian law that set important parameters on decision-making by financial institutions.

Part C

discusses additional approaches that financial institutions can take as part of their human rights due diligence to strengthen their decision-making and better manage risk to their clients and to their own institutions.





Financial institutions (FIs) have a responsibility to respect human rights, which includes identifying and taking action in relation to impacts with which their portfolio companies are involved. This responsibility is set out in the UN Guiding Principles on Business and Human Rights (UNGPs) and the OECD Guidelines on Multinational Enterprises and it is reflected in the policies to which most leading financial institutions have committed themselves (see Box 1). These international standards have been incorporated into national laws, and explicitly underpin a new wave of regulation on

the responsibility of business enterprises, including the Corporate Sustainability Due Diligence Directive and Corporate Sustainability Reporting Directive in Europe.¹

The responsibility includes undertaking human rights due diligence (HRDD) to address impacts associated with portfolio companies. This also makes smart business sense: severe impacts on people frequently create financial, legal, reputational and business opportunity risks for clients, which often translate into credit and other business risks for the financial institution.

Box 1

The International Standards: The UN Guiding Principles and the OECD Guidelines

The **UN Guiding Principles on Business and Human Rights (UNGPs)** are the authoritative global standard for preventing and addressing human rights harms linked to business activity. Endorsed by the UN Human Rights Council in 2011, they apply to all states and all companies.

The UNGPs rest on three pillars:

- 1. The State duty to protect** people from human rights abuse by third parties, including businesses.
- 2. The corporate responsibility to respect** human rights, including through human rights due diligence to identify, prevent and address impacts on people.

- 3. Access to remedy** for individuals and communities harmed by business activity.

The OECD Guidelines for Multinational Enterprises on Responsible Business Conduct are aligned with the UNGPs and incorporate their human rights standards. The OECD provides additional practical guidance on how companies - including investors and lenders - should carry out due diligence to identify, prevent and address impacts across their operations, value chains and business relationships.

For financial institutions, this means assessing and addressing human rights risks connected not only to their own operations but also to the activities of **portfolio companies, clients and transactions**.

¹ Risks (and impacts) are then assessed in reference to international and regional conventions and commentary.

A. The Challenges



Financial institutions that undertake HRDD in the defense and dual-use technology space face a complex set of structural, technical and governance challenges. Based on our conversations with sustainability and compliance practitioners within investors and lenders, four key challenges stand out.



Challenge 1

There can be a strategic tension between policy objectives and sustainability commitments

Practitioners that we speak to are receptive to demands from governments, management and clients to support important imperatives of national and regional security, conflict readiness and defense capacity-building. At the same time, they seek to continue to play their mandated role to safeguard their institutions' commitments and responsibilities to avoid involvement in the most severe human rights risks. The pressure to revisit traditional red-lines has never been greater, from increased NATO spending mandates to the growth of publicly-backed finance vehicles, to amended weapons and defense exclusion policies amongst investors and banks.

Concurrently, there has been a concerted effort to connect rearmament and defense spending with a moral imperative. Debate continues as to whether defense-related assets have a home in sustainable fund products, including SFDR Article 8 (and even 9) funds - or not.² Yet geopolitical contexts rarely remain stable. Policies or engagement rationales shaped by the perceived legitimacy of one conflict may quickly be tested as new conflicts emerge, alliances shift, and/or the actors involved change.



Challenge 2

HRDD on weapons and dual-use technologies can stretch the institution's technical capacity

Financial institutions struggle to **navigate opaque end-use pathways** for portfolio company products, services and platforms. This opacity makes it difficult to determine where, how and by whom weapons or dual-use technologies are ultimately deployed. Practitioners in sustainability and compliance functions are aware that too often the institution lacks internal expertise on defense-related supply chains and/or the sort of technical mechanisms that might avoid and mitigate harm, as well as how international humanitarian law (IHL) relates to specific forms of conflicts, combatants and weapons. They recognise that this limits the ability of the institution to engage credibly with clients.

Sustainability practitioners also cite confusion about **threshold and scope criteria for their policies and exclusion criteria**, including:

- how to define a “weapon” or a “weapons company”,
- how to treat suppliers of essential components,
- which components are critical to weapon systems,
- how to treat those who broker weapons systems or their components, and
- how to define, and where to draw boundaries around, dual-use technologies.

Moreover recent analysis (e.g. ESG Book³) shows that defense-related risks extend well beyond traditional manufacturers to ‘quiet enablers’ such as real estate and infrastructure, **for example through the provision of facilities, land and logistics that support defense activities**. This underscores that due diligence must move beyond a narrow focus on weapons producers to encompass the broader ecosystem of financing and support.

² At the time of writing, the European Commission is reviewing the Sustainable Finance Disclosure Regulation (SFDR) as part of the expected “SFDR 2.0” reforms. Proposed changes include a move toward a product-labelling framework that may replace the current Article 6/8/9 disclosure categories. As part of this process, asset managers are reassessing the positioning of existing Article 8 and 9 funds, including the treatment of sectors such as defense, in light of evolving regulatory expectations and ongoing policy debates around sustainable finance and European security priorities.”

³ ESG Book, proprietary analysis shared via ESG Book newsletter; see www.esgbook.com.



Challenge 3

Companies involved in weapons and dual-use tech can be difficult to engage

Even where the technical capacity exists to ask the right due diligence questions, weapons-related companies can still be difficult to engage. Investors and lenders seeking to have conversations about impacts on people can find it difficult to get the attention of target companies, and at times have struggled to get them to disclose their customers or ultimate end users. The clients/investees concerned may cite national security constraints, classified contracting and related security clearance requirements. There is a sense among sustainability practitioners that even where these constraints don't exist, large technology companies in particular appear not to feel a commercial imperative to engage with financiers, or provide limited access and information when they do.

Recent debates around advanced technologies demonstrate, however, that national security priorities do not automatically resolve responsible-use questions. Even where governments invoke security imperatives, companies themselves have sometimes resisted proposals that would weaken safeguards on the development of powerful technologies.



Challenge 4

The complexity of due diligence in the weapons and dual-use tech field is amplified when it intersects with existing weaknesses in bank due diligence

Some investors - and many lenders - have been vocal in regulatory debates about the challenges of conducting due diligence on social risks associated with the downstream sale and use of their clients' products and services (though, self-published examples suggest that the picture is rather more optimistic).

What is more certain, however, is the fact that banks place considerably **more emphasis on their upfront due diligence** in client KYC ("Know Your Customer") checks/screening and onboarding than on **ongoing** due diligence of existing clients and their activities and relationships. This invariably leads to the risk that institutions **miss potential impacts on people that arise as contexts evolve**.

This also has implications for any decision to increase **financing to defense-related start-ups**. The FT laments that defense start-ups are "struggling to access credit despite many of the region's biggest banks relaxing restrictions on lending to the sector." However, this would arguably require a significant improvement in post-onboarding HRDD within FIs. A hallmark of a start-up is often that key elements of the business model - specific product technology, distribution channels and customers or end-users - are, if not undetermined, evolving and subject to flux. These aspects are precisely what can trigger heightened human rights risk. However most banks would need to make improvements to due diligence processes to nimbly identify and address this changing risk profile after onboarding.



B. Anchors in Heightened Human Rights Due Diligence and International Humanitarian Law



 “Even wars have limits.”
Jean Pictet

Through our work with investors and lenders we engage regularly with the challenges outlined above. These issues rarely admit simple answers. This section highlights some **anchors** - areas of foundational clarity that remain stable even in a dynamic environment – that help provide boundaries on appropriate decision-making and keep financial institutions on track for effective risk management.

Financial institutions can begin their analysis with established international standards that are already familiar to sustainability practitioners. The UNGPs emphasize that when assessing risks to people in conflict-affected contexts, companies should apply heightened HRDD and consider IHL alongside international human rights law.



Anchor 1

The severity of harms associated with weapons and dual-use technologies warrants their prioritization in human rights due diligence.

A key challenge for portfolio-based institutions is one of scale - that is, how to address the numerous impacts to which they are connected by virtue of their financing (See Box 3 below). Here the international standards

provide a pragmatic solution: where necessary, HRDD may be prioritized such that it is applied first in those general areas of a portfolio - by sector, geography, client type and other factors - where impacts are mostly likely to be severe. As noted above, involvement with these impacts tends also to be a source of particular risk to financial institutions themselves.

Few impacts are as severe as those associated with weapons and dual use technology. As such, it is right that many FIs determine that defense-related⁴ clients, investees and transactions ought to be prioritized for heightened due diligence - even where portfolio exposure is limited. For example, Barclays explicitly identifies weapons and dual-use technology exports as a salient human rights risk⁵, while several other banks - including [ABN AMRO](#), [ING](#) and [Unicredit](#) - address arms-related risks within their environmental and social risk frameworks or sector policies.



Anchor 2

International humanitarian law provides a neutral and widely recognised foundation for defense-related due diligence.

IHL comprises the body of international law that regulates the conduct of parties in an armed conflict. It is reflected most prominently in the four Geneva Conventions and their Additional Protocols⁶ and so-called ‘customary IHL’. These laws include rules on the protection of civilians and restrictions on the means and methods of warfare.

⁴ It is important to note that this extends beyond a traditional sector focus: The UN Working Group definition of the "arms sector" refers to "the full value chain of actors producing or being directly linked to the research, development, design, production, delivery, maintenance, repair and overhaul of military weapons systems, subsystems, parts, components, and ancillary equipment. This includes actors providing 'technical assistance, training, financial or other assistance, related to military activities or the provision, maintenance or use of any arms and related material'". See Responsible business conduct in the arms sector: Ensuring business practice in line with the UN Guiding Principles on Business and Human Rights at <https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf>

⁵ See, for example, Barclays PLC’s salient issue “Weapons and Dual Use Technology” reported in their [2023 Annual Report](#) (p. 241): “Technologies associated with the Defense and Security sector are continuously developing. This includes advancements such as autonomous weapons and dual use technology which could be used in a multitude of applications including in weapons and surveillance technology. Weapons and dual use technologies, if misused, have the potential to cause some of the most severe human rights violations, in particular, in the context of repressive state action or conflict.”

⁶ See the rules contained in ICRC Customary IHL database as describing and presenting the current state of customary IHL: <https://ihl-databases.icrc.org/en/customary-ihl>

A select number of financial institutions explicitly anchor their defense sector policies in IHL or closely related legal standards. For example, [La Banque Postale](#), [ABN AMRO](#) and [BNP Paribas](#) in Europe, as well as [DBS](#) in Asia, reference IHL or “humanitarian principles” rooted in IHL, humanitarian disarmament treaties (such as those prohibiting cluster munitions and anti-personnel mines), or related international conventions when setting financing criteria and due diligence expectations. We are also aware of institutions seeking legal advice on IHL from external counsel for specific clients and transactions.

It is precisely in situations of political complexity that the neutral principles of the laws of armed conflict become most critical. Reference to established laws of armed conflict can have the effect of **depoliticising discussions** within financial institutions and with clients.

However, outside of select examples, there is a general [lack of IHL awareness in the financial sector](#). The International Committee of the Red Cross (ICRC) in Australia has also noted, for example, that since Australian financial institutions often take a “risk-averse approach” to investing in countries in conflict, this has given rise to a “perception that IHL is not relevant to those [financial] institutions’ operations”. This can leave institutions underprepared when links to armed conflict inevitably arise within their portfolios.



Anchor 3

International humanitarian law applies irrespective of the legitimacy of the conflict or the conduct of the opposing party.

Sustainability practitioners within institutions have at times found themselves in internal debates about whether the constraints imposed by international humanitarian law should carry the same weight when nations are defending themselves against an aggressor - particularly one that does not itself respect the laws of war. To be sure, nation states have a right to legitimate self-defense, including where their territorial integrity has been breached by an aggressor. However, an aggressor’s conduct does not cancel out IHL obligations.

IHL applies irrespective of whether a state is acting in self-defense and binds all parties to a conflict - allies and adversaries alike. The body of law was specifically designed to apply in situations of armed conflict - including where one party does not comply - in order to preserve minimum protections for civilians, and to limit the means and methods of warfare.

The experience with weapons such as anti-personnel landmines illustrates why these constraints exist: their use has been widely prohibited under international treaty law in part because of their persistent and disproportionate impact on civilians. The Landmine Monitor consistently reports that civilians account for the large majority of recorded landmine casualties globally: in 2024, [90% of casualties were civilian and half were children](#). For financial institutions, (even those with internal mandates to focus on excluding only the worst cases), the relevant question is therefore not whether humanitarian law should yield to military necessity; rather, it is how to identify and restrict the flow of capital to the manufacture, distribution and use of weapons that may disproportionately or indiscriminately harm civilians or other non-combatants. This is a line that must be held if the core humanitarian purpose of the laws of armed conflict is to be preserved in practice, and if financial institutions are to give meaningful effect to the human rights commitments they have publicly embraced.



Anchor 4

Overly narrow weapons exclusions can create blind spots in defense-related risk assessment

In the current geopolitical environment, some financial institutions are revisiting or diluting longstanding weapons exclusions in order to facilitate capital flows to defense activities associated with particular conflicts. Yet such policy adjustments rarely remain confined to a single geopolitical context. Once exclusions are relaxed, institutions must apply the same policies across their portfolios - potentially exposing them to defense-related activities linked to other conflicts they may be less willing to support. More importantly, history shows that weapons systems, technologies and supply chains rarely remain confined to a single theatre of conflict. Capabilities developed or financed in one conflict frequently [migrate into others](#), underscoring the risks of narrowing institutional risk lenses in response to a specific geopolitical moment.

In the investment space in particular, political pressure, [regulatory retrenchment](#) and the profitability of the defense sector is encouraging some institutions to [dilute longstanding controversial weapons exclusions](#). This produces what the Heartland Initiative calls a “patchwork of inconsistency” and a dangerous narrowing of the risk lens.

For example, by focusing only on formally prohibited weapons (rather than the broader universe of controversial weapons) under the EU’s Paris-aligned Benchmark (PAB) and Climate Transition Benchmark

(CTB) rules, capital providers risk missing fast-moving indicators of heightened risk. This is particularly pertinent in relation to autonomous and AI-enabled systems, creating what Heartland describes as a “massive fiduciary blind spot.”⁷



Anchor 5

Emerging defense technologies remain subject to the core principles of IHL

Indeed, international humanitarian law continues to be interpreted and applied in light of emerging defense and dual-use technologies, including increasingly autonomous weapons systems⁸. IHL does not prohibit autonomy in weapons per se. It does, however, establish clear constraints that are highly relevant for financial institutions’ due diligence on these technologies. In particular, weapons that are by nature incapable of being used in compliance with the principles of ‘distinction’, ‘proportionality’ and ‘precaution’ in the context of a military attack are understood to raise acute legal and human rights concerns.

Reflecting this, several states and expert bodies, including the International Committee for the Red Cross, have called for strict limits and, in some cases, prohibitions, on autonomous weapons systems that lack meaningful human control (and pose complex questions of legal liability). For banks and investors, this points to the following minimum guardrails:

- a. Heightened scrutiny of companies developing or supplying highly autonomous weapons capabilities;
- b. Caution where end-use contexts present a high risk of indiscriminate effects; and
- c. Clear exclusion of financing for weapons that are inherently indiscriminate or otherwise prohibited under international law.



Anchor 6

Connections to armed conflict may create legal exposure for financial institutions and their decision-makers

Concrete legal risks arise for businesses and individual corporate actors, including directors, executives and other decision-makers, in circumstances where their activities are ‘closely linked’ to an armed conflict. The International Committee of the Red Cross has warned, for example, that if a bank were to facilitate payments by one party to a party participating in an armed conflict which uses those payments to fund their military operations, this may be considered ‘closely linked’ in the context of IHL.

⁷ There is no universally accepted definition of “controversial weapons.” The term does not appear in international humanitarian law, which instead regulates specific categories of weapons through dedicated treaties—such as anti-personnel mines, cluster munitions, chemical weapons and biological weapons. In practice, financial institutions and ESG data providers apply their own definitions of the category, often drawing on these treaties. Moreover, as technology evolves, careful due diligence is needed to identify, for example, where weapons platforms may be rendered controversial by the integration of sophisticated software packages.

⁸ There is currently no settled international legal definition of lethal autonomous weapons systems (LAWS), nor a specific treaty instrument comprehensively regulating them. The International Committee of the Red Cross (ICRC) has proposed a widely cited working definition, describing an autonomous weapon system as one “designed to select and engage one or more targets without the need for human intervention after activation” (see ICRC, *Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects*, available at <https://www.icrc.org/en/document/autonomous-weapon-systems>). In his July 2024 report summarising state and expert views on LAWS, the UN Secretary-General noted broad concern regarding the degree of human involvement in the identification, classification, interception and engagement of targets, with several States emphasising that merely nominal human input — meaning actions that do not materially affect autonomous target selection or engagement — would be insufficient (see UN Secretary-General, *Lethal Autonomous Weapons Systems*, July 2024, available via <https://documents.un.org>).

Box 2

There are few, but powerful, examples in which the front line of financial institutions has faced judicial and quasi-judicial scrutiny for alleged links to serious conflict-related harms. Notably, BNP Paribas has been subject to ongoing U.S. litigation concerning its provision of financial services to the Sudanese government during the Darfur conflict, while cases such as Jesner v. Arab Bank and civil society analyses of banking activity in Israeli settlements illustrate the growing willingness of

courts and stakeholders to test financial institutions' potential exposure to international humanitarian law-related risks. More recently, Norges Bank Investment Management has faced sustained scrutiny in Norway, including a 2026 criminal complaint alleging that the Oil Fund's investments in certain companies may contribute to IHL crimes in Gaza, underscoring the increased public scrutiny of investor responsibilities in conflict-affected contexts.





C. Key approaches for navigating the currents based on judgement and evolving practice

Front-line teams in financial institutions understandably seek clarity in a complicated area. Within the bright lines that are provided by IHL, as discussed above, financial institutions still have to navigate areas where considerable judgement is required.

In our work with investors and lenders evaluating specific transactions or portfolio companies, several practical implications of the international standards on business and human rights (notably the UNGPs and the OECD Guidelines) consistently prove useful. This final section outlines six approaches, providing reference sources, resources and examples. Box 3 provides some specific background on relevant concepts in the UNGPs, for readers that are less familiar with these.



Approach 1

Assess potential impacts on people across the full value chain and lifecycle of weapons systems, and consider the capacity of the company to manage these

The international standards take a full value chain approach. A financier providing capital (or insurance, or export credit) in a weapons - or dual-use-related transaction may therefore be connected to impacts on people through aspects such as the design, distribution and end-use or lifecycle of the products being financed.

HRDD on relevant companies should also be informed by an understanding of the lifecycle of the relevant weapons systems. This includes considering impacts associated with:

- known or likely end-users;
- research and development (including battle testing);
- the design and deployment of dual-use products; and
- risks of diversion of weapons⁹ (whether within or beyond a given conflict).

Importantly, the investor or lender should consider the **company's commitment and capacity to avoid or mitigate these risks** as they continue to evolve, beyond intentions expressed in policies. This requires examining both the company's understanding of these risks and its capacity to manage them. In practice, this includes assessing:

- drivers of risk within the business model, such as speed in development, engaging in business relationships with limited influence over end-users and the inherent risks of products that can cause harm if misused; and
- the quality of the portfolio company's own human rights due diligence, including its identification of its own salient human rights issues and the quality of its stakeholder engagement.

This can be resource-intensive research. This data is often not readily available within data sets that can be bought. However, it is typically an appropriate allocation of resources when institutions elect to incorporate these higher risk companies in their portfolio.



Approach 2

Determine whether your financing creates a connection to harm

Connection between an investor or lender and an impact on people requires, at minimum, a *direct linkage* between the financing provided and the operations, products or services associated with the harm (See Box 3).

General purposes/wholesale lending or equity investment **connects the lender or investor to all activities** of the company receiving finance, including any weapons-related activities. However, the investor or lender is not likely to be connected to impacts associated with the company's weapons business if, for example, its financing is limited to a transaction involving another product line. As such, the use of specific purpose transactions and ring-fencing to avoid contributing capital to weapons-related activities

⁹ That is, the risk that weapons are transferred, captured, stolen, or otherwise end up in the hands of unintended or unauthorized users.

can indicate that there is no connection between the financier and an impact.

However, lenders should note that any such presumption of non-connection remains rebuttable based on the

facts.¹⁰ In higher risk cases, investors and lenders may wish to assess whether firms have safeguards in place to prevent data leakage between commercial and defense applications when both operate within the same company.

Box 3

Cause, Contribution and Direct Linkage: Forms of Involvement with Human Rights Harm

Under the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct, companies - including financial institutions - can be involved with (or connected to) adverse human rights impacts in three different ways.

- **Cause:** A company **causes** harm where its own activities directly result in an adverse impact on people. For example, where a financial institution discriminates against employees or customers in its own operations. In such cases, the company must cease the activity, prevent recurrence and provide remedy.
- **Contribution:** A company **contributes** to harm where its actions help enable, incentivize or facilitate the harmful conduct of another party. For example, where a lender structures financing in a way that incentivizes or enables a client to proceed with an activity known to pose severe human rights risks. In such cases, the company must cease its contribution, use its **leverage** to mitigate remaining impacts, and provide remedy to the extent of its contribution.

- **Direct linkage:** A company may also be **directly linked** to harm through its business relationships, even where it has not caused or contributed to the impact itself. For example, where an investor or lender provides capital to a company whose products or operations cause harm to people. In these cases, the institution is expected to **use its leverage to prevent or mitigate the harm**, including through engagement with the client or investee.

For **financial institutions**, involvement in portfolio company impacts will most often arise through **direct linkage**, since investors and lenders typically provide capital rather than directly controlling operations. However, this position is not static. As noted by the Office of the UN High Commissioner for Human Rights, where a financial institution **should have known of risks through effective due diligence but failed to take reasonable action**, its involvement may shift from linkage to **contribution**.

This is why effective **human rights due diligence and use of leverage** are critical in preventing and addressing harms connected to investments and financing relationships.

¹⁰ See OECD, *Due Diligence Guidance for Responsible Business Conduct* (2018) and OECD, *Due Diligence for Responsible Corporate Lending and Securities Underwriting* (2019).

Banks' client onboarding and KYC systems often flag risks - albeit predominantly risks to the financial institution - associated with corporate groups. However, under the international standards **the institution will not (in principle) be connected to a weapons-producing company by virtue of financing another company in the corporate group.** Shared corporate governance may rebut this presumption of separation and warrant deeper investigation. Moreover, there may be important policy and reputational reasons for the institution to take a more conservative approach to a group.

Regardless, while risks of connection to human rights harms may only be a sub-set of risks flagged by KYC systems, care should be taken not to falsely narrow the understanding of risks by using overly rigid thresholds and distinctions. Institutions sometimes establish **thresholds** to manage complexity - for example limiting enhanced due diligence to companies where weapons-related activities represent a certain share of revenue. But while such thresholds may be useful for operational purposes, they do not eliminate responsibility under the international standards where severe risks to people are foreseeable and ought to have been prioritised.

Similarly, while institutions sometimes seek comfort in distinctions between “defensive” and “offensive” technologies, international humanitarian law does not draw such clear lines. The legality of weapons turns instead on their characteristics and use, and due diligence should take into account the fact that technologies can readily be adapted or repurposed across contexts.



Approach 3

Build and use leverage to influence portfolio company conduct

Investors and lenders are expected to use **leverage** (that is, influence), with portfolio companies when the institution is connected to harm via their investment/financing. As noted above, companies involved in weapons and dual-use technology can be difficult to engage. However, we have seen the following approaches demonstrate some traction.

- Some institutions have explored **time-stamping** key due diligence decisions - that is, formally recording the information available, risk assessment and rationale at the point of financing - in an effort to

strengthen internal discipline, create a clear audit trail and support ongoing or mandatorily updated monitoring.

- Others have used **ring-fencing** (discussed above) to distance financing from certain activities and/or end-users within a client's product portfolio and, at times, to send a message about what their capital is prepared to support.
- **Asking questions** can be a key use of leverage by providers of capital, as it signals scrutiny, shapes management attention and creates incentives for improved human rights performance. Questions about responsible design¹¹, for example, are recommended by experts, including as leading indicators of responsible deployment.



Approach 4

Understand when to consider divestment and the consequences of staying engaged

As noted above, there are instances where the ability to influence actors associated with weapons and dual-use technology is difficult. However, a lack of leverage over a portfolio company - including an inability to achieve an adequate response to HRDD lines of enquiry - **does not provide a shield to responsibility for harms** under the international standards.

Importantly, **the more serious the harm, the faster the institution will need to see change** before considering divestment. Credible reports of violations of international humanitarian and human rights law (such as from the UN, international legal bodies and credible journalistic sources) should be taken as signals of harm of the utmost seriousness.

If the institution chooses to stay in the relationship with a portfolio company involved with these types of harms, it will need to accept the legal, reputational and other direct business risks of doing so.

Institutions that do not use sufficient leverage with portfolio companies - particularly where there are signs of severe human rights harms - risk finding themselves in a situation of **contribution to harm** under the international standards, further raising the business risks they face and triggering responsibilities to provide or participate in **remedy**.

¹¹ Responsibility by design is “the idea that ethical and legal compliance must be integrated from the earliest stage of development, through the entire AI system lifecycle as well as in the socio-technical institutions in which AI applications are embedded”. See further GC REIM, Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain (2025) at <https://hcass.nl/report/gc-reaim-responsible-by-design-strategic-guidance-report/>



Approach 5

Understand that government involvement, including via financing initiatives and export control regimes, does not obviate an institution's human rights due diligence responsibilities

The responsibility of financial institutions under the international standards to identify, prevent, mitigate and account for impacts on people with which they are involved, exists independently of government duties and applies whether or not governments are able or willing to exercise their duties appropriately.

Consider a bank financing a client or transaction involving the relocation of a large community for the purpose of an infrastructure project. Financiers already know that they cannot rely entirely on government assurances about land tenure rights and will need to conduct deeper due diligence where there are reasonable grounds to do so. In the same way, when it comes to companies involved in defense-related activities, there is a need to consider the risk of products or services being used in ways that impact human rights or breach IHL, be it in the hands of traditional military allies of their home state or otherwise.

As such, participation in government-led initiatives for defense financing aimed at mobilizing private capital to the sector at scale do not provide a fail-safe that removes the need for due diligence. **For example, institutions participating in and partnering with the proposed Defence, Security and Resilience Bank, or the European Defence Equity Initiative, retain their own due diligence responsibilities and will still be connected to impacts associated with their financing.**

Similarly, export licensing regimes do not provide a basis for by-passing due diligence. For portfolio companies that are subject to the EU Corporate Sustainability Due Diligence Directive (CSDDD), it is true that the requirements to conduct mandatory downstream due diligence for arms and related products are limited if those products are already subject to export controls.¹² It is also true that state-based export control regimes in the EU and the US reference human rights and IHL considerations. However, as noted above, the genesis of the corporate responsibility to respect was an acknowledgement that nation states do not always meet their duty to protect from human rights harms, for reasons ranging from a lack of political will to corruption.

Human rights considerations under export control regimes, the UNGPs and the CSDDD do not represent competing standards; if FIs and their clients conduct due diligence in accordance with the international standards it should be viewed as strengthening safeguards reflected in governments' commitments to prevent export of items that can or will be misused.

Moreover, anecdotal evidence from companies we work with suggests that where a client company can provide information to export control authorities on the company's own due diligence efforts, this can support their case for receiving an export license, and builds trust with the authority.



Approach 6

Maintain institutional capacity that is sufficient for effective defense-related due diligence

Ultimately, financial institutions will be judged on their transparency, governance, and the nature and quality of their due diligence.

Institutions must maintain sufficiently robust governance to address the inevitable challenges that arise in this dynamic and complex area.

Further, as we have navigated these challenges with investors and lenders, one aspect becomes strikingly clear: **the more that institutions choose to incorporate higher risk defense-related companies and transactions into their portfolios, the more that sustainability and legal and compliance teams must be appropriately resourced.** This resourcing must be commensurate to meet some of the most complex challenges of downstream HRDD.

Failure to provide governance structure and support, budget and headcount to enable this critical task means that financial institutions will simply end up failing to manage some of the most acute human rights risks in their portfolios, and the related risks to their own business.

¹² See Recital 25 and Article 3(1)(g).

Conclusion



“War does not determine who is right — only who is left.”

Bertrand Russell

Financial institutions are navigating defense-related finance at a moment of profound geopolitical turbulence, marked by multiplying conflicts, rapid technological change and growing pressure to support national security priorities. At the same time, the sector is confronting powerful incentives to provide this financing: expanding defense markets present lucrative opportunities, governments are encouraging greater flows of capital to defense-related activities, and some institutions perceive themselves as partially insulated from risk where financing aligns with geopolitical priorities. Moreover, practitioners within institutions have expressed a genuine desire to direct capital to self-defense activities that are widely seen as legitimate. These dynamics create genuine challenges for senior management, as well as sustainability and risk teams seeking to apply international standards in practice.

Yet these pressures do not alter the underlying reality: decisions about financing defense-related activities are

ultimately decisions about risks to people. In a context where the consequences of those decisions can be irreversible, short-term recalibrations of policy - whether to capture opportunity or respond to political signals - risk weakening precisely the guardrails designed to limit harm. In doing so, they may expose institutions to the significant systemic, financial, legal, and reputational risks that arise from their association with those impacts.

The analysis above demonstrates that the international standards provide a valuable and practical framework for navigating these complexities. By anchoring their approaches in the core principles of international humanitarian law and the UN Guiding Principles, and by applying careful judgement in areas where practice continues to evolve, financial institutions can conduct due diligence that addresses risks to people - and to themselves.

While there are no simple answers in this space, anchoring decision-making in established principles supports investors and lenders to remain aligned with the commitments they have made to respect people’s rights in the way they do business. It is precisely in moments such as these that consistent and disciplined application of the standards - and the resourcing required to deliver this in practice - matters most.

Box 4 Further reading

- An investor-led **Principles for Responsible Defense Investment** initiative is currently under development, aimed at helping investors apply existing human rights and responsible investment standards to defense-related exposures. A [concept note](#) is available and a draft framework is expected in 2026 following an ongoing consultation process.
- In May 2023, the Responsible Investment Association Australasia (RIAA) released its [Investor Toolkit on Human Rights and Armed Conflict](#) – one of the first guides written by investors for investors on the topic.
- A 2023 [ICRC Humanitarian Law & Policy Blog article](#) by Kurnadi (Australian Red Cross) and international lawyer Sinclair-Blakemore examines the growing relevance of IHL for the financial sector.
- The IEEE SA Industry Connections Research Group on Issues of Autonomy and AI in Defense Systems has created a [Framework For Human Decision-Making Through the Lifecycle of Autonomous and Intelligent Systems in Defense Applications \(2024\)](#). The framework provides “a granular means for identifying the technical considerations that are necessary to meet legal requirements, to inform and guide ethical discussions, and to determine human responsibility and accountability across the entire lifecycle of autonomous and intelligent systems”.

About **Shift**

Shift is a non-profit, mission-driven organization working globally to embed respect for human rights into business. We leverage the UN Guiding Principles on Business and Human Rights to shape the standards, incentives and practices that are needed for a fairer economic system in which everyone, not just the few, can thrive.

Visit shiftproject.org and follow us at [@shiftproject](https://twitter.com/shiftproject).

Weapons, Dual Use tech and Financial Institutions

Shift, New York. April 2026
© 2026 Shift Project, Ltd.