

GRID

GUIDANCE FOR RESPONSIBLE INVESTMENT
IN DEFENCE-RELATED COMPANIES

LONDON CONSULTATION DRAFT
INVESTOR GUIDANCE

V0.1

JULY 2026

Contents

1. INTRODUCTION	7
The defence ecosystem	8
2. MANAGER DUE DILIGENCE & ENGAGEMENT	10
Introduction	10
Understanding the asset owner objective	10
Exclusions lists	11
Managers’ management of defence sector risk	11
Example questions for asset owners to ask	12
Calibrating questions to the objective	13
Calibrating manager due diligence across asset classes	13
3. EXCLUSIONARY SCREENING	14
Setting screening criteria	15
‘Norms-based’ exclusionary screening	15
Controversial weapons	16
Revenue threshold screening	18
Geographic Screens	18
Data providers.....	20
Next steps.....	20
4. OPERATIONALISING EXPECTATIONS FOR DEFENCE RELATED COMPANIES	21
5. PORTFOLIO DUE DILIGENCE.....	24
Key messages	24
Prioritising controversies.....	25
Prioritising the most significant defence exposures across all manager holdings..	26
Prioritising holdings at the sub-portfolio (fund/strategy level)	27
Prioritising conflict-affected and high-risk area exposure	29
Towards a Risk-Based Prioritisation Framework	31
6. DUE DILIGENCE FOR PRIORITY REVIEW COMPANIES – PART A – CONTEXT	33
Understanding the company context	33
7. DUE DILIGENCE FOR PRIORITY REVIEW COMPANIES – PART B – COMPANY POLICIES, PROCESSES & RISK MANAGEMENT	40

Human rights commitment and governance	41
Risk identification and prioritisation	41
Due diligence in Commercial and Export Decisions	42
Product- and Technology-specific safeguards	42
Transparency, Stakeholder Engagement and Accountability	43
8. INTEGRATION IN FUND DECISION MAKING	44
9. PRE-INVESTMENT DUE DILIGENCE	48
Introduction	48
Understanding outputs	49
Next steps	49
10. NAVIGATING CONTROVERSIES (INCLUDING RESPONSIBLE DIVESTMENT)	50
Introduction	50
Supporting tools	50
Understanding types of controversies	51
Assessing severity	51
Further analysis	52
Investor responses	52
Controversy related divestment	53
11. ENGAGEMENT	54
Company Engagement	54
Scope, proportionality and constraints	54
Using engagement questions to assess robustness and transparency	55
Example engagement questions tailored to defence-related companies	55
Engagement as an ongoing and proportionate process	55
Escalation	56
Engaging with the defence ecosystem: dialogue with public authorities and industry bodies	56
Practical Guidance	57
12. COMMUNICATING TO CLIENTS AND STAKEHOLDERS	58
Appendix 1: Definitions	62
Appendix 2: Case Studies	65
Investor Example - LBP AM's approach to integrating company-level human rights due diligence into investment analysis	65

Dialogue with public authorities and industry bodies example - France	67
Appendix 3: Investors – Understanding Yourself	70
Appendix 4: Data providers approaches to controversial weapons.....	71
Appendix 5: Basis for different elements of controversial weapons definition	73
Appendix 6: Setting business thresholds in exclusions	75
Appendix 7: Due diligence tools	77
A. Company defence-related revenue	77
B. Defence-related products and services.....	78
C. Geographic footprint and CAHRA exposure	80
D. Applicable regulatory and legal frameworks	81
E. Customers, end-users and business relationships.....	83
F. Controversies.....	84
Risk management and mitigation	85
G. Assessing company policies.....	86
H. Assessing company processes	87
Next steps	89
Appendix 8: Engagement questions for companies.....	90
Appendix 9: Factors to bear in mind in assessing arms export regimes	92

EXECUTIVE SUMMARY

[to be completed for general send out]

1. INTRODUCTION

Background - GRID responds to an urgent need for a framework to help investors navigate the challenges of investing in defence-related companies. This initiative does not try to reconcile the irreconcilable given the diversity of investor perspectives. It recognises the legitimacy of choosing not to invest in defence-related companies, and at the same time supports the potential for investors to invest responsibly in defence-related companies within an appropriate framework.

The drivers for the creation of GRID are numerous: a growing push by states to increase investment in the defence sector in response to increased geopolitical tension; the evolving and increasingly fluid definition of what constitutes a defence investment, with major technology firms and startups increasingly engaging in defence-related activities; and the challenge of demonstrating responsible business conduct in a sector whose products and services are often used in armed conflict, whose clients are frequently domestic or foreign governments and where the system itself shields the sector from rigorous investor scrutiny.

Acknowledging the ongoing efforts to enhance responsible business conduct across the defence value chain and in relation to investments in conflict-affected and high-risk areas, GRID has a strong focus on downstream risks associated with product use and potential misuse. This reflects the growing materiality of these risks for investors, and the notable absence of guidance in this area.

Consultation Draft Guidance - This Guidance will form the core of the GRID document and is designed to follow the Expectations Chapter for defence companies (which is the other Chapter being reviewed in the initial round of consultations).

The Guidance should be adaptable to the specific investor context, but it is recognised that more bespoke tools and guidance may be needed for certain contexts. With the broad range of investors and their use cases, there is no ‘one-size fits all’ for responsible investment in defence-related companies. Instead, there are multiple tools and approaches which are relevant to different investors. As such, while the Guidance has been designed to be adaptable to specific contexts, it is also intended to be modular. For example, where an investor only wishes to implement an exclusionary approach, that section can be viewed in relative isolation, while another investor with a very concentrated portfolio may only want to focus on company due diligence. There is no requirement to integrate or adopt the Guidance or Expectations in their entirety and GRID is not mandating investors take specific actions. An investor’s use of one section does not necessarily indicate its support, adoption or endorsement of all the guidance provided by GRID.

Scope – GRID aims to help investors bring responsible investment principles to defence-related investments. The Guidance chapter does not attempt to answer the question of whether defence-related investments can be categorised as ethical, sustainable or

positive impact investments. It is intended to be equally helpful to those who believe defence-related investment is a positive or necessary force (for example as an enabling condition that advances SDG 16 Peace, Justice and Strong Institutions, is necessary to defend democracies, and helps to create a world in which sustainable finance supports all necessary parts of the economic system) as it is to those who take markedly different views. There is a broad and legitimate spectrum of investor approaches to defence and the GRID focus is to help investors navigate different sorts of defence-related risks. GRID's role is not to place investments in or outside of a specific taxonomy or point of view; the guiding star for GRID remains international humanitarian law and the UN Guiding Principles on Business and Human Rights.

The following sections explain how investors can operationalise the GRID Expectations on companies, how to approach manager due diligence and engagement, key considerations for exclusionary approaches and how to integrate defence-considerations for 'in-fund decision making' such as ESG weightings. It considers portfolio wide due diligence (understanding exposure), before narrowing down to company due diligence (understanding actual or potential investments) and how well companies are aligned with the GRID Expectations. This leads to a section guiding investors on engagement with defence-related companies and considerations on how to deal with significant controversies. It closes out with advice on how to communicate to clients and stakeholders on these issues.

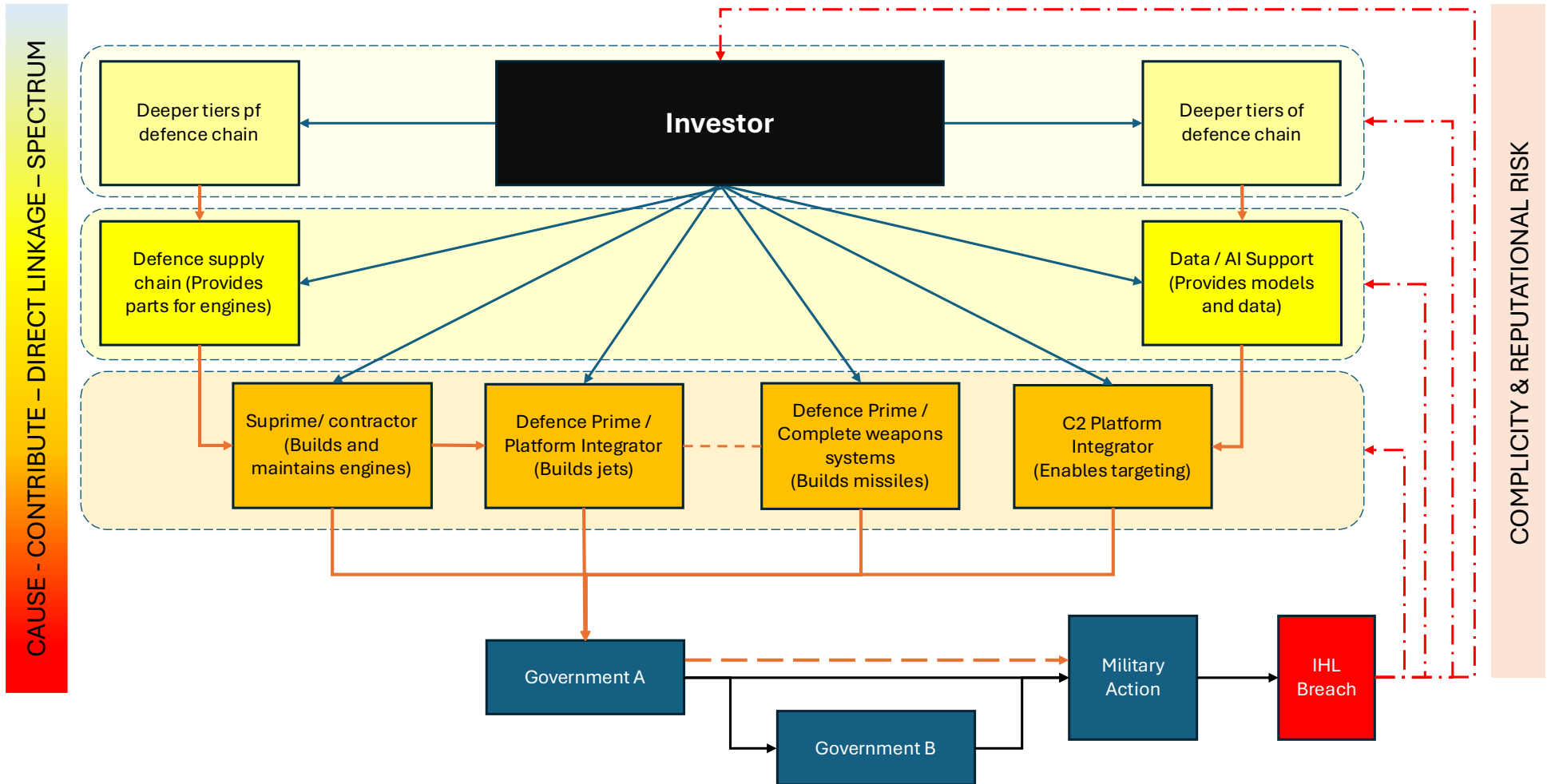
Once finalised, the expectations and guidance sections will be combined in a final document, which will include an overview of the risks investors face in defence-related company investments as well as the broader context. That introduction will build on the content of the [Concept Note](#) which launched the GRID work and should be seen as a companion to this document.

The defence ecosystem

The image below is the GRID overview of the ecosystem for defence related companies based on their connections to government, military action and potential adverse impacts, as well as the feedback loops for complicity and reputational risks and the cause-contribute-linkage spectrum under the UNGPs.

The 'closer' companies are to military action, the more likely they are to be causing or contributing to adverse human rights impacts. However, complicity risks and particularly reputational risks are not necessarily reduced by being further away from adverse impacts.

This framework can be relevant to the settings of any exclusionary screens that investors wish to adopt and may also be relevant to what is an adequate response to the investor expectations set out in the relevant chapter and as context for any engagement activity. The defence ecosystem will be expanded on in the Context section of the final Guidance.



2. MANAGER DUE DILIGENCE & ENGAGEMENT

This section is focused on asset owners and asset managers who allocate capital to other Asset Managers and in particular where capital allocators rely on managers to implement responsible investment practices (including human rights due diligence) on their behalf.

Introduction

Asset owners can communicate expectations on defence-related investments to asset managers through policies, mandates, side letters and engagement. Due diligence is a mechanism through which asset managers can implement those expectations in practice.

In the defence context, manager due diligence raises specific challenges as defence-related risks are:

- Highly context-dependent;
- Often concentrated downstream (through end-use, misuse or diversion of products and services); and
- Shaped by factors outside the direct control of investors, including government export decisions and national security considerations.

In practice, due diligence questions on defence are typically not asked in isolation. They are often embedded within broader ESG, human rights, or exclusion-focused questionnaires and frameworks, and tend to focus on exposure to military contracting, defence revenue, controversial weapons and operations in CAHRA (across sectors rather than specifically in defence).

Understanding the asset owner objective

In practice, asset owner questions on defence tend to reflect three distinct objectives:

1. **Confirming exclusions** – ensuring policies (e.g. controversial weapons, military contracting) have not been breached.
2. **Responding to member/beneficiary queries** – explaining specific holdings, often triggered by NGO reports, media, or UN databases.
3. **Understanding broader exposure** – assessing how managers identify and manage broad exposure to risk associated with defence (e.g. dual-use, indirect exposure, CAHRA), how they interpret and exercise judgment, and how they deploy different tools in practice (screening, engagement, escalation).

The first two are now well embedded in market practice. The third is less consistently addressed – and where there is an opportunity for more decision-useful due diligence that can add value.

Exclusions lists

Exclusion lists are important tools for many investors. However, lists provide binary outputs and limited insight into the broader management of risk. The use of exclusion lists in relation to the defence sector can be challenging given the variety of companies that have, or may in the future have, links to the sector, including new and developing technologies. *See section 3 below for considerations when setting and implementing exclusionary screens.*

A combined or more nuanced approach would take into account the broader defence related exposure, the manager's approaches to dealing with it and any unintended consequences which may arise from divestment decisions where disengagement does not improve or may actively harm outcomes on the ground.

Managers' management of defence sector risk

Where the objective is to understand exposure more deeply, due diligence should focus less on whether exposure exists in a manager's portfolio, and more on how it is interpreted, assessed and managed in practice. In the defence context, this means assessing whether the manager can:

- Distinguish between prohibited weapons, conventional defence activities and dual use exposure;
- Identify where exposure creates elevated human rights or conflict-related risks;
- Apply a clear and consistent decision framework (e.g. when to exclude, avoid, engage, escalate or divest); and
- Demonstrate ongoing management of risk, rather than relying solely on point-in-time screening.

It is important that due diligence questions test governance, process, judgement and action, rather than outputs alone. This includes understanding:

- How defence exposure is defined and classified by the manager, including distinctions between controversial, conventional and dual-use activities;
- How external lists and databases¹ are used in their analysis – as inputs rather than endpoints – and how their limitations are understood;
- How risk is assessed in context, including end-use, customer exposure, geography and governance controls;

¹ These could include outputs from data providers, such as lists of 'norms breach companies', reports from civil society (such as benchmarks and rankings, or SIPRI's Arms Industry Database), government lists (such as the US list of entities identified as Chinese Military Companies), or lists from intergovernmental bodies such as the UN Human Rights Office database of businesses involved in Israeli settlements in the occupied West Bank.

- How exposure is actively managed over time, particularly through engagement and escalation where concerns persist or arise during the holding period; and
- How decisions are made and applied consistently and defensibly, especially in sensitive or high-profile situations.

Example questions for asset owners to ask

The following questions are designed to test framework quality and decision-making, rather than just manager policy positions. Asset owners may wish to explore these questions as part of their manager due diligence or ongoing engagement. There are relatively generic, but it is recognised that some owners and managers may take different approaches (such as supplying their own exclusion lists for public equity managers to implement, rather than relying on the manager to implement an exclusion policy).

Topic	Question for Manager
<i>Framing and definitions</i>	• How do you define defence exposure for responsible investment purposes? • How do you distinguish between: ○ prohibited / controversial weapons, ○ conventional defence activities, ○ dual-use technologies, ○ and broader security-related services?
<i>Screening and exclusions</i>	• What exclusions apply, and where do you rely on case-by-case assessment instead? • How were these thresholds or exclusions determined?
<i>Risk assessment</i>	• How do you assess whether defence-related activities create elevated human rights, conflict-related, or IHL risks? • How do you consider: end-use and end-user, customer base, geographic exposure, and governance controls?
<i>Decision-making framework</i>	• What factors determine whether you exclude, avoid investment, engage, escalate, or divest?
<i>Deal structuring</i>	• Do you actively structure deal terms, shareholder agreements, or governance vetoes to minimise the risk of foreseeable product misuse or unethical downstream military contracting?
<i>Consistency and governance</i>	• How do you ensure decisions are consistent across portfolios, evidence-based, and defensible, particularly in politically sensitive contexts?

Calibrating questions to the objective

The depth of manager due diligence should reflect what the asset owner is trying to achieve:

- Compliance-focused → screening and exclusion confirmation
- Stakeholder response → company-level explanations and transparency
- Risk management → deeper, framework-based questions

Being explicit about this objective helps ensure due diligence is proportionate and focused.

Calibrating manager due diligence across asset classes

Recognising the different types of exposure, holding periods and potential leverage, the approach to manager due diligence will need to be tailored to each asset class:

In **listed equities and liquid fixed income**, where portfolios change frequently and allow for rapid divestment, asset owners should evaluate how regularly managers engage with companies and monitor evolving situations and whether they have structured, time-bound escalation frameworks when downstream risks escalate.

Conversely, for **sovereign bonds and macro-fixed income**, asset owners should evaluate whether and how the manager is assessing country-level governance, including whether the issuing state is a signatory to international arms control treaties, and evaluating their broader domestic framework for export control compliance.

In contrast, asset owners assessing **private markets or illiquid asset managers** should look for rigorous, pre-investment heightened human rights due diligence (hHRDD) embedded directly into the deal assessment process—particularly for early-stage dual-use technology firms, including software and AI, where end-use profiles are highly speculative. Whilst these managers may have limited ability to divest, they do have contractual leverage and ongoing ability to engage.

3. EXCLUSIONARY SCREENING

This section addresses defence-related investment exclusions which may be set either by the asset owner or by the asset manager. While the asset owner is more likely to determine an overarching entity-wide policy, the manager is likely to have a product-by-product approach informed by the investment thesis of the product in question. This section is relevant to both asset owners and asset managers; for ease of reference, "investor" is used throughout to mean both owners and managers. It covers investor justifications for setting exclusion criteria, norms based and IHL related screens, business involvement screening, revenue threshold screening and geographic screens.² This section also considers the role of ESG data providers in screening.

Exclusionary screening ("screening"³) is a common approach that allows investors to set rules on permissible investments, based on defined criteria such as company sector, activity/revenue source, ESG risks or conduct.

The Guidance does not mandate nor preclude exclusionary screens of sectors or specific companies, and it is important that investors consider their fiduciary duties when adopting any voluntary restriction of the assets they invest in and seek to understand any positive or negative impact it may have upon financial performance, alongside all the other considerations referred to in this guidance.

See section 9 'Navigating controversies' for responsible divestment considerations.

Note on Exclusions and Access to Capital - Responsible investment exclusions (and 'ESG' or 'ethical' investing in general) are not thought to have had a material impact on the wider defence industry's access to capital. There have been genuine problems for small and medium sized defence businesses in terms of access to capital and banking services, but these are more due to issues with defence procurement and banking regulation and requirements than responsible investment. See [Are ESG Standards the Scapegoat for Stalling Defence Growth? | Royal United Services Institute](#) for more details.

² For further details, see *An introduction to responsible investment: Screening and exclusions*, Principle for Responsible Investment <https://www.unpri.org/deep-dive?id=an-introduction-to-responsible-investment-screening-and-exclusions> (accessible to PRI members only).

³ Positive screening or best-in class screening is not considered in this section, but 'in-fund management' covers aspects of this element of screening in section XX.

Setting screening criteria

The increased blurring of lines between defence and technology companies and the proportion of the investible universe connected in some way with defence create challenges for investors who want to ‘avoid defence’ while meeting their fiduciary duties.

Each investor will have a unique combination of fiduciary duties, client requirements and stakeholder expectations, all set within the context of international business and human rights standards. An investor’s approach to exclusionary screens should take into account each of these factors.

When investors independently implement exclusionary screens and wish to align with the Guidance, they are recommended to:

- Be able to clearly define what is meant by ‘defence’, ‘military contracting’ or ‘weapons’ for the purpose of any exclusions;
- Set out their approach in a policy document;
- Clearly justify their approach, including whether exclusions are on ethical grounds or client requirements, for financial, legal and reputational risk reasons, as part of fund criteria, or to avoid involvement in companies that are connected with serious human rights risks and impacts;
- Ensure the approach is appropriate for their specific portfolio, resourcing capacity and – realistically – the data and systems which they have access to in order to deliver on their policy commitments;
- Consider a combination of the following elements (further detailed in this section) when deciding on an approach:
 - Norms-breach / norms-based exclusions
 - Screens relating to business activities which are higher risks from for IHL violations (e.g. Controversial Weapons)
 - Revenue threshold screening based on defence related business activities
 - Geographic screening

‘Norms-based’ exclusionary screening

Investors wishing to exclude companies on the basis of ‘norms breaches’ (usually by reference to international business and human rights standards including the UN Guiding Principles on Business and Human Rights, the OECD Guidelines and the UN Global Compact 10 Principles) should be aware of the challenges inherent in this approach.

"Breaches" of norms can be difficult to identify; for example, a "breach" may cover a spectrum ranging from a lack of aligned policies to a finding of violation by an OECD National Contact Point.

Data providers that asset managers rely on to flag companies in breach of human rights norms take different approaches to identifying and assessing companies and frequently do not consider the downstream use of defence products and services when making assessments, while others do not consider certain areas of conflict. Reliance on data providers for pre-emptive screens may miss the most significant norms breaches depending on the scope of the data provider research⁴.

Controversial weapons

There is no universal definition of ‘controversial weapons’, but they are generally understood to include weapons which do not align with international humanitarian law, for example due to their indiscriminate nature or which cause unnecessary suffering. Many States prohibit certain controversial weapons but investor portfolios likely have exposure to companies whose operations and supply chains are in countries with different prohibitions. The production, transfer, stockpiling and use of such weapons may expose companies and investors to significant legal (civil and criminal), regulatory, financial, operational, and reputational risks, given the severe humanitarian consequences associated with such weapons and the international and domestic laws controlling them⁵.

The GRID Expectations are clear that companies should avoid involvement in weapons prohibited by customary IHL, or by the IHL Treaties signed by their country of domicile, or which would involve their operations or supply chains in other countries - or employees who are citizens of other countries - breaching any treaties those countries have signed.

Investors should recognise the inherent risks relating to controversial weapons and are recommended to have processes in place to understand and navigate (and where necessary avoid) the risks of exposure to companies involved in the manufacture or support of such products. Where investors have exclusionary screens as part of their investment approach, companies involved in controversial weapons are recommended to be the starting point⁶.

Note on ESG data providers - ESG data providers are well placed to support investors by the provision of ‘controversial weapons’ data. These products

⁴ The Investor Initiative on Human Rights Data (II-HRD) has developed guidance for ESG Data Providers on assessing companies in relation to non-compliance with, and breaches of, international human rights norms and is engaging with Data Providers on their products: [ii-hrd-report-september-2025.pdf](https://www.ii-hrd.org/ii-hrd-report-september-2025.pdf)

⁵ The manufacture and transfer of parts and components of prohibited weapons can breach specific weapons prohibitions in international law and can also, where transferred, constitute unlawful aid or assistance in the breach of prohibitions applicable to other States (See e.g. *Treaty on the Prohibition on Nuclear Weapons*, art. 1; *Anti-Personnel Mine Ban Convention* art. 1; *Cluster munitions convention* art. 1; *Arms Trade Treaty* art. 6(2); *ARSIWA* art. 16) which in certain circumstances can entail individual criminal responsibility (See e.g. *Chemical Weapons Convention* art. VII; *Treaty on the Prohibition on Nuclear Weapons*, art. 5(2); *Anti-Personnel Mine Ban Convention* art. 9; *Cluster Munitions Convention* art. 9; *Biological Weapons Convention* art. IV).

⁶ See [Financial Exclusions tracker](#) for a review of different investor exclusions

are generally binary for revenue data (i.e. the company is assessed as making either 0% or >0% revenue from various controversial weapons), although this figure can often be estimated. Companies are regularly divided by data providers into two groups based on whether their products and services are ‘tailor made and essential’ for the lethal use of the weapon or ‘non-tailor made or non-essential’ for lethal use. More details of ESG Data Provider approaches to Controversial Weapons screening can be seen in Appendix 4.

Investors developing exclusions relating to controversial weapons should be informed by their own context (such as their tolerance for inherent human rights or reputational risks and the treaties which their country of domicile have ratified). *Appendix 5: Basis for different elements of controversial weapons definition*, has been developed to assist investors in deciding an appropriate approach for their specific context as it relates to weapons which are considered controversial or are prohibited.

Note on nuclear weapons – Investors have taken a variety of exclusionary approaches to companies producing or involved in the development, maintenance and deployment of nuclear weapons, reflecting its controversial nature. The Non-Proliferation Treaty (NPT) and the Treaty Prohibiting Nuclear Weapons (TPNW) are both relevant international treaties for investors to consider. While the TPNW prohibits the production, stockpiling, use and threat of use of nuclear weapons, it is only applicable to the parties (which do not include the five recognised nuclear weapons states under the NPT, the non-NPT states who have nuclear weapons, or any members of NATO). As such, the TPNW is binding on many states, but it is not customary IHL. The ICJ Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons (1996) found that while the threat or use of nuclear weapons would generally be contrary to IHL they could not conclude definitely whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake⁷.

Investors will have to decide for themselves on the most appropriate approach to nuclear weapons-linked companies, but it will likely rest on a combination of their specific mandates, fund aims, national context and approach to defence and human rights in general. Investors are encouraged to consider how they take a consistent or differentiated approach based on the locations of their businesses, offices, clients and beneficiaries (as they relate to both the NPT and TPNW).

⁷ See <https://casebook.icrc.org/case-study/icj-nuclear-weapons-advisory-opinion> for more details

Revenue threshold screening

Beyond the controversial weapons categorised above, there are a broad range of defence related business activities (products and services) which investors may wish to screen for.

Investors may exclude companies that derive revenue from defence-related activities above a defined threshold. Thresholds can range from 0% exposure to higher levels, intended to exclude only companies for which defence is a material part of the business.

Revenue-based screens are often used to differentiate between companies whose primary business is defence-related and those with only limited exposure through diversified activities.

Appendix 6: Setting business thresholds in exclusions provides further guidance.

Geographic Screens

Investors may have a view that certain countries present inherently greater risks when considering companies in terms of their domicile and the destination of their products and services, which may be managed in part through geographic exclusions.

As an example, in Europe, multiple investors have recently set out revised approaches to defence exclusions, noting the pressure to improve European security and resilience. But in the absence of any geographic boundaries, these changes have the potential to additionally drive capital towards companies that – at best - have no role in supporting European security and which – at worst – may have an active role in undermining European security. Investing in the defence sector of certain countries has the potential to significantly increase the human rights and reputational risks the investor faces.

Mandatory sanctions regimes administered by bodies such as the UN Security Council, the European Union or national governments will effectively pre-determine certain geographic exclusions as a matter of legal compliance, and investors should treat these as a floor rather than a ceiling for geographic risk assessment. It is also the case that export licensing criteria vary between jurisdictions. Where a company's geographic footprint includes countries with materially weaker export control environments, investors may wish to apply a lower revenue threshold or require more intensive due diligence as part of their geographic screening approach, rather than treating all non-sanctioned geographies as equivalent.

Countries allegedly engaged in internal oppression and international crimes (acts of aggression, war crimes, crimes against humanity and genocide) may also have a domestic defence sector which enables these activities (and the risk increases that those regimes enable those same activities in third countries through lax export regimes).

Adding geographies to exclusion screens may be conceptually challenging for investors who have preferred to take a politically neutral stance. But investors who have explained

their willingness to invest in defence in terms of supporting the security of their clients/client countries risk accusations of ‘defence washing’ if they ignore geopolitical realities or allegations of misuse.

Investors are therefore recommended to establish and be able to explain any geographic boundaries for their exclusions. In developing these boundaries, investors can consider issues including:

- Relevant sanction lists (e.g. UN, national) ;
- Client mandates or geographies relevant for ‘supporting security’;
- Metrics of internal oppression such as civil, political and religious freedoms;
- Levels of corruption / resilience to corruption within the country⁸; and
- Allegations of international crimes

Investors should also recognise that geography-based restrictions may be more fluid and need to be revisited more often than other factors.

EXAMPLE BOX – An investor has a client base in one European country who have asked for a fund that supports European security and resilience. The investor implements a screen that:

- Does not exclude defence-related companies from the EU or UK or Norway.
- Has a 2% revenue threshold for companies from its sovereign-debt exclusion list (which is itself built on the presence of sanctions, and corruption and freedom scores).
- Has a 10% revenue threshold for companies from all other countries.
- Has a 0% threshold on all domestically prohibited weapons (in this case, companies making revenue from chemical, biological weapons, anti-personnel mines and cluster munitions, as well as nuclear weapons not covered by the Non-Proliferation Treaty).

8 Various external resources are available to help gauge risks, including:

- War Watch (World Assessment and Tracking of Civilian Harm) [Explore - WAR WATCH](#)
- Transparency International’s Corruption Perceptions Index: [Corruption Perceptions Index 2025 - Transparency.org](#)
- CIVICUS Monitor’s People Power under Attack [Global Findings 2025 - Civicus Monitor](#)

Data providers

ESG data providers are key actors in the exclusionary screening process as they can provide cost effective data at a scale sufficient to implement screens on large investible universes. They can manage screening on behalf of clients or provide the data for in-house use by investors or managers. However, the data provider *definitions* then become a critical deciding factor on which companies are screened in and out of an investment universe. It is vital to understand the alignment between the intent of the investor policy and the data provider methodology and capacity.

As such, investors are recommended to explore data provider methodologies in depth to understand how different types of products and services are treated by the provider and how that maps to the investor's own red lines. The outcomes of a screening exercise can result in exclusion lists which significantly differ based on the chosen data provider.

Two of the key data providers are MSCI and Sustainalytics. [MSCI Business Involvement Screening Research Methodology](#) and [Sustainalytics Product Involvement Methodology](#).

Next steps

Initial screens can help investors establish clear boundaries and prioritise resources. It should however be viewed as a starting point rather than an endpoint. Companies that pass exclusionary screens may still be linked to severe human rights and IHL risks through their products, services, business relationships or customers. Investors should therefore consider whether further human rights due diligence is required, particularly where defence-related activities create heightened risks of adverse impacts.

4. OPERATIONALISING EXPECTATIONS FOR DEFENCE RELATED COMPANIES

This section outlines how investors can translate their policies into consistent investment decisions, by setting and communicating expectations for potential investee companies. These expectations are usually conveyed and operationalised on behalf of asset owners by asset managers. The role of asset managers is addressed further in section [xx].

Defence-related companies operating in line with GRID should avoid legal complicity, respect human rights, act ethically and eliminate bribery and corruption, and they should implement robust policies and processes throughout their business to manage their related legal, reputational, human rights and financial risks. Further details are set out in the Expectations chapter (separate document).

Investors should set an internal policy on their approach to the risks involved in defence-sector investing, which will take into account what they expect of their underlying investments. GRID has not set out a template policy, but Appendix 3 provides a list of considerations which investors may find useful in understanding their own unique context prior to any policy discussions.

To help manage their own financial, human rights, legal and reputational risks, investors can operationalise these expectations on companies through actions such as:

- Internally agree on the GRID Expectations, or equivalent expectations, so that the investor has a common point of reference for all defence-related companies and investment activities. These expectations also ensure that any decision making or escalation is based on a consistent framework.
 - o Noting that the GRID Expectations are grounded in responsible business conduct (RBC) norms, investors may elect not to set out specific defence-related expectations if they already have overarching RBC expectations (such as an expectation for all companies to implement the OECD Guidelines and UNGPs throughout their value chain). However, given the specific risks concerning defence-related companies including downstream risks typically not addressed by general frameworks, investors may choose to supplement general RBC expectations with more detailed expectations for companies with defence or military involvement, for example, a formal commitment to integrating international humanitarian law (IHL) into their own policy commitments and due diligence processes.
- At a high level, integrate expectations into a policy or position statement. Where possible, this should be public to support the wider expectation-setting on defence related companies.

- Where internal policies are not feasible, investors may consider joint public statements or support for industry positions which confirm the expectations on investees.
- Communicate expectations to defence-related companies.
 - What ‘communication’ looks like in practice will differ depending on the type of investor. For instance, Norges Bank Investment Management (NBIM) is globally known as having significant holdings in most large, listed companies. NBIM’s public Expectations⁹ are more likely to be noticed by a company than a position statement from a small pension fund or asset manager.
 - Direct communication to all public holdings may not be practical, but expectations can be communicated via available channels, for example:
 - Pre or post voting communications with companies
 - Specific engagements e.g. letters to management
 - Public statements or escalation activities
 - In private markets, asset managers are expected to communicate directly to potential investee companies, appropriate to the stage of the company and the levels of ownership and influence.
 - For pre-seed or seed-stage companies, managers should push for expectations to be integrated into company policies or approaches and in board / founder discussions to ensure RBC is integrated at the start, not bolted on when risks manifest, or to address regulatory concerns. Developing internal or external expertise in human rights, international humanitarian law and international criminal law is essential, but may take time and may not be feasible for seed/pre-seed companies. It is important to take an elevated view and not default to minimum regulatory compliance advice.
 - For Series A-E / pre-IPO companies and in private equity buyouts, investors should ensure that companies translate expectations into tangible commitments to governance, policies and processes within term sheets, shareholders’ agreements, articles of association and/or reserved matters. This will ensure that risk management frameworks are appropriately governed and resourced prior to any IPO or sale.
 - Asset managers with other private markets strategies – including private credit – should use the influence they have to seek to ensure

⁹ [Our expectations | Norges Bank Investment Management](#)

that their expectations have been appropriately communicated to portfolio companies.

- Focus should be given to ensuring that companies understand areas of highest risk, including complicity in breaches of IHL or IHRL.
- Managers may support companies in develop appropriate strategies for risk management, drawing on credible public tools¹⁰. Investors may also highlight in their policy statements particular resources which align with their preferred approach.
- Communicate expectations to managers - Asset owners and managers who invest via/with other managers should consider:
 - Actively communicate expectations of defence related companies to their managers.
 - Set expectations for managers themselves to appropriately manage the financial, human rights, reputational and legal risks from defence related companies on behalf of their clients.
 - How this is implemented will depend on the nature of the relationship between investors and their managers (for example, through side letters, contracts, investment management agreements, manager frameworks, workshops and capacity building).

¹⁰ See FINAL USEFUL REFERENCE SECTION (e.g. [7-indicators-of-corp-best-prac-final-2021.pdf](#))

5. PORTFOLIO DUE DILIGENCE

This section considers how asset managers can approach their portfolios to understand their exposures, risks and subsequent actions relating to defence-related investments. While targeted at asset managers, elements will also be relevant to certain asset owners – both in terms of actions which they conduct ‘in-house’ and where actions are devolved to managers. There is no one-size-fits-all approach that can be recommended, but four approaches are set out based on different priorities (controversies, most significant financial exposure across all manager holdings, key exposures at the sub-portfolio level, and conflict / high-risk exposures). Investors may wish to use one, some, or all of these techniques, depending on their portfolio, resources and focus. Company due diligence is expanded on in the following section, which can be informed by the portfolio due diligence.

Key messages

For most investors, conducting an in-depth assessment of every defence company within a portfolio or investment universe is unlikely to be feasible. Portfolio size, resource constraints, data availability and differing investment strategies often require investors to make decisions regarding where to focus their due diligence efforts. Prioritisation is therefore both a practical necessity and a central feature of a risk-based approach to responsible business conduct.

The OECD Guidelines for Multinational Enterprises and related OECD due diligence guidance recognise that investors will frequently need to prioritise investee companies and risks. In doing so, the primary consideration should be the severity and likelihood of adverse impacts, particularly where investors are seeking to identify situations in which human rights or international humanitarian law (IHL) risks are most significant. At the same time, investors may also consider factors such as the nature of their relationship with an investee company, the importance of the investment within the portfolio, and their ability to exercise leverage or influence outcomes.

There is, however, no single approach to prioritisation. The appropriate methodology will depend on an investor’s investment strategy, responsible investment objectives, available resources and stewardship and exclusion approach. A large asset manager with diversified holdings may initially focus on identifying higher-risk sectors, activities or geographies across an entire portfolio. Other investors may choose to focus on specific themes, such as exposure to conflict-affected and high-risk areas, controversial weapons, or military surveillance technologies. Investors with concentrated portfolios and significant holdings may be able to undertake a more detailed company-level assessments from the outset, whereas others may need to adopt a more gradual, tiered process.

The objective of prioritisation is to ensure that finite resources are directed towards those areas where adverse impacts are most likely to be severe, where companies are most

exposed to heightened human rights or IHL risks, or where investors consider that they can most effectively contribute to improved outcomes. The following section proposes a number of approaches that investors may use to identify and prioritise defence companies for more detailed due diligence, depending on their objectives, investment philosophy, and stewardship capacity. The final section summarises the pros and cons of the four approaches.

Prioritising controversies

Many investors currently rely, at least in part, on controversy monitoring and ESG data providers as an entry point for identifying potential human rights risks within the defence industry. Controversy screening can undoubtedly play an important role in a due diligence process. It may help identify emerging concerns, support engagement decisions, highlight areas requiring further investigation and provide useful signals regarding potential weaknesses in a company's risk management framework.

However, controversy-based approaches are generally insufficient as a standalone methodology for prioritising human rights due diligence in the defence industry and are best understood as a complement to a broader risk-based assessment.

First, controversy screening is inherently dependent on the methodologies, coverage and underlying assumptions of ESG data providers. These methodologies can vary considerably in terms of scope, thresholds and sources. Certain providers may place significant emphasis on corruption, environmental incidents or governance failures, while providing limited coverage of conflict-related risks, downstream due diligence practices or the deployment of products in conflict-affected and high-risk areas (CAHRAs). Equally, complex issues such as end-use risks, customer due diligence, export control practices or a company's potential contribution to adverse impacts through its products and services are often difficult to capture through standard controversy frameworks. As a result, investors relying exclusively on controversy data may inadvertently overlook areas that are highly relevant from a human rights or IHL perspective.

Second, controversy-based approaches are fundamentally reactive. In most cases, a company becomes the subject of a controversy because adverse impacts have allegedly already occurred, or because allegations have become sufficiently visible to attract media, civil society, regulatory or public attention. By the time a controversy is identified and reflected in ESG datasets, the underlying human rights harm may already have materialised and, in some cases, become difficult to prevent or mitigate. From a responsible business conduct perspective, this can limit investors' ability to engage proactively with companies, encourage the strengthening of due diligence processes before harm occurs, or contribute meaningfully to efforts to prevent, mitigate or remedy adverse impacts.

Third, controversy screening may provide a fragmented and potentially distorted picture of sector-wide risks. Public attention often focuses on a limited number of companies, technologies, countries or conflicts, while other actors facing comparable or even greater risks may receive little scrutiny. Visibility can depend on a range of factors, including media attention, civil society capacity, data availability or geopolitical sensitivities, rather than the severity of underlying risks alone. Consequently, controversy-based approaches may concentrate investor attention on a small number of well-known companies while providing limited insight into broader patterns of risk across the defence sector, value chains or peer groups.

Perhaps most importantly, controversies tend to identify where problems have already emerged rather than where risks are most significant. As such, they do not necessarily support a comprehensive assessment of a company's exposure to potential adverse impacts, nor do they enable investors to compare companies consistently across a portfolio or investment universe. Investors seeking to align their activities with the OECD's risk-based due diligence framework may therefore benefit from complementing controversy monitoring with more systematic approaches that consider factors such as defence exposure, product characteristics, position within the value chain and exposure to conflict-affected and high-risk areas.

For these reasons, controversy monitoring may be more effective when integrated into a broader prioritisation framework. The following approaches provide complementary ways of identifying companies and situations that may warrant enhanced scrutiny, including before significant adverse impacts or public controversies emerge.

Prioritising the most significant defence exposures across all manager holdings

A second approach to prioritisation consists of identifying the investee companies that represent the most significant defence-related exposure across an investor's portfolio. This approach reflects the reality that many investors, particularly those with diversified portfolios, may not have the resources to conduct detailed human rights due diligence on every defence-related holding. Instead, they may choose to focus initially on the companies that are most significant, both from an investment perspective and from an exposure to defence activities perspective.

In practice, this typically involves combining two dimensions. The first is financial significance, including factors such as the size of the holding, concentration of assets under management (AUM), portfolio weighting, or the strategic importance of the investment within the portfolio. The second is operational exposure to defence activities, including involvement in weapons systems, military equipment, defence services, dual-use technologies with military applications, surveillance technologies, cybersecurity, aerospace, artificial intelligence, intelligence support, logistics, maintenance and training activities supporting military operations.

Under this approach, companies that combine substantial portfolio exposure with significant involvement in defence activities would be prioritised for enhanced human rights and IHL risk assessments. The underlying rationale is that these companies are likely to have the greatest influence on the overall defence-related risk profile of the portfolio and may therefore warrant more detailed scrutiny and engagement.

This approach may be particularly appropriate for investors with a relatively concentrated exposure to the defence sector, where a small number of companies account for a significant proportion of defence-related assets. It may also be relevant where responsible investment teams face resource constraints and must decide where enhanced due diligence is most likely to generate meaningful insights or stewardship outcomes. Similarly, it can serve as a practical starting point for investors seeking to build expertise on defence-related risks by focusing first on large, established defence companies, with substantial defence revenues and global operations.

One of the principal advantages of this approach is its close alignment within existing portfolio management practices. Most investors already monitor portfolio concentrations, material holdings and sector exposures, making the approach relatively straightforward to operationalise using available holdings data and public company disclosures. It also provides a clear basis for prioritising stewardship activities and efforts towards issues that are likely to be of greatest significance, from both a financial and defence-related perspective.

At the same time, investors should be aware of the limitations of such an approach. Financial significance does not necessarily correlate with the severity of potential human rights or IHL impacts. Smaller holdings may be involved in highly sensitive products, technologies or activities that present elevated risks despite representing only a limited proportion of portfolio assets. Likewise, companies operating in particularly sensitive conflict environments or supplying niche capabilities linked to acute human rights concerns may not be identified through an exposure-based screening alone. As a result, this approach is often most effective when used as an initial prioritisation tool, complemented by additional assessments that consider product-specific, geographical and conflict-related factors.

Prioritising holdings at the sub-portfolio (fund/strategy level)

A third approach to prioritisation consists of assessing risk at the sub-portfolio, fund or investment strategy level, before focusing on individual companies. Rather than seeking to identify the most significant defence-related holdings across the entire asset manager holdings, this methodology starts by determining which funds, mandates or investment strategies are structurally exposed to defence-related activities and the associated human rights and IHL risks. Those can then be prioritised for more detailed analysis, including company-level screening and enhanced due diligence.

This approach is particularly well suited to asset managers overseeing large and diversified investment universes, where defence exposure may be concentrated within specific strategies rather than across the entire organisation. For example, exposure may be found within dedicated aerospace and defence funds, security-related investment themes, infrastructure strategies, industrial portfolios or broader equity mandates with a significant allocation to defence and security companies. By first identifying those funds, mandates or strategies where defence-related risks are most likely to arise, investors can target their efforts more efficiently and embed human rights due diligence into existing investment processes.

In practice, such an assessment may draw on a combination of internal sector classifications, revenue-based screening tools, ESG risk mapping frameworks, human rights risk assessments and thematic allocations. The objective is not only to identify companies involved in defence activities, but also to understand where defence-related human rights and humanitarian risks are concentrated within the investment platform. Once priority funds have been identified, investors can undertake a more granular review of constituent companies using the contextual lenses and human rights due diligence tools described hereafter.

This methodology presents several advantages. First, it enables a more systematic and scalable approach to due diligence by focusing attention on segments of the portfolio that are structurally more exposed to defence-related risks. It can also help investors identify cumulative or systemic patterns that may not be apparent through a company-by-company assessment. For example, a portfolio may contain multiple companies exposed to the same conflict-affected region, military customer base or category of higher-risk technology. Reviewing those exposures collectively may provide a more comprehensive understanding of the portfolio's overall risk profile.

A portfolio-based approach can also help align human rights due diligence with investment decision-making processes. By integrating defence-related risk considerations into portfolio construction, monitoring and review mechanisms, investors may be better positioned to identify potential concerns before adverse impacts materialise. It further encourages a broader assessment of a company's responsible business conduct profile, rather than focusing exclusively on individual controversies or allegations. In this respect, the methodology can support a more forward-looking and risk-based approach that is consistent with the OECD's emphasis on identifying and prioritising the most significant risks of adverse impacts.

Another advantage is that it allows investors to focus on companies presenting the most material risks from an investor perspective, based on a consistent set of criteria applied across a portfolio or strategy. This can help ensure that prioritisation decisions remain grounded in a structured risk assessment process, rather than being driven primarily by public attention, media scrutiny or isolated event.

However, this approach also has limitations. Portfolio-level screening may not always capture indirect exposures that arise through complex supply chains, minority shareholdings, or specialised technologies integrated into broader defence systems. Depending on the breadth of the portfolios selected, it may also generate a large universe of companies requiring further assessment, potentially stretching available resources. Effective implementation therefore relies on robust data, analytical tools and internal expertise to ensure that prioritisation remains meaningful over time.

Furthermore, while portfolio-level assessments are effective at identifying structural patterns of risk, they may be less sensitive to rapidly evolving developments in specific conflict situations or to emerging controversies involving individual companies. As a result, investors may wish to complement this methodology with more targeted monitoring of conflict-affected and high-risk areas, significant geopolitical developments and company-specific incidents that could materially alter the risk profile of a holding.

For investors seeking to establish a scalable and consistent framework for defence-related human rights due diligence, portfolio-level prioritisation can therefore provide an effective entry point. It allows for resources to be directed towards those parts of the investment universe where risks are most likely to arise, while creating a structured basis for subsequent company-level analysis and engagement.

Prioritising conflict-affected and high-risk area exposure

A fourth approach consists of prioritising due diligence based on exposure to specific conflict-affected and high-risk areas (CAHRAs), rather than on portfolio composition or the financial significance of individual holdings. Under this methodology, investors begin by identifying conflict situations, military operations, occupations or other high-risk contexts that are associated with heightened risks of severe human rights abuses or violations of IHL. They then assess which companies are allegedly or demonstrably connected to those situations through their products, services, technologies or business relationships.

Unlike the previous approaches, which are primarily driven by investment exposure, this methodology is grounded in the severity of potential impacts. Screening typically relies on external and independent sources, including reports from civil society organisations, UN bodies, panels of experts, special rapporteurs, academic research, investigative journalism, forensic investigations, and specialised databases tracking corporate involvement in conflict situations. Companies identified as supplying products, technologies or services linked to specific conflicts, military campaigns, occupations or internal security operations may then be prioritised for enhanced human rights due diligence, irrespective of the size of the investor's holding or the company's weight within a portfolio.

This approach may be particularly relevant where investors seek to align their due diligence efforts closely within international human rights and humanitarian law

expectations. It can be especially valuable in situations involving risks of severe adverse impacts, such as allegations of war crimes, civilian harm, violations of the laws of armed conflict, repression of civilian populations or prolonged occupations. Likewise, it may provide a useful framework during periods of conflict escalation or in rapidly deteriorating security environments, where investors need to identify and assess emerging risks in a timely manner.

One of the principal strengths of this methodology is its strong alignment with the OECD's severity-based approach to prioritisation. By focusing attention on situations where adverse impacts are potentially most serious, investors can ensure that due diligence resources are directed towards areas where the consequences for affected individuals and communities may be greatest. This approach also enables investors to develop a more nuanced understanding of defence-related human rights risks by grounding their analysis in specific conflict situations rather than relying solely on abstract risk indicators. Examining how companies and their products are connected to real-world contexts can help build internal expertise, improve risk identification and strengthen engagement strategies.

A further advantage is that this approach can support earlier intervention. Monitoring conflict situations, allegations and emerging concerns may allow investors to identify potential risks before they translate into significant legal, operational or reputational challenges for companies. It is also often closely aligned with the expectations of stakeholders, including clients and beneficiaries, civil society organisations, who may be particularly concerned with situations involving severe human rights impacts or significant humanitarian consequences.

However, investors should also be aware of the limitations of this methodology. Its effectiveness depends heavily on the availability, quality and timeliness of external reporting. In some contexts, information may be incomplete, contested or difficult to verify, while in others the absence of reporting should not automatically be interpreted as the absence of risk. Investors choosing to conduct their own research may also face significant resource requirements and technical challenges.

In addition, this approach is often inherently reactive, as it frequently relies on conflict allegations or incidents that have already been documented. As a result, it may be less effective at identifying risks before they materialise. It can also provide a narrower perspective than portfolio-wide or company-wide assessments, as the focus on specific contexts may overlook other parts of the portfolio that present material defence-related human rights risks, but are not currently associated with a particular conflict or controversy.

Finally, because conflict situations are often politically sensitive, investors may face perceptions of politicisation when selecting particular conflicts, countries or allegations for heightened scrutiny. Clear governance processes, transparent selection criteria and reliance on credible external sources can therefore play an important role in ensuring that

prioritisation decisions remain consistent, objective and aligned with responsible business conduct expectations.

For investors whose primary objective is to identify and respond to the most severe risks of adverse impacts, a CAHRA-focused approach can provide a valuable complement to portfolio-level and company-level prioritisation methodologies. By focusing attention on concrete situations where human rights and IHL risks are most acute, it helps ensure that due diligence efforts remain anchored in the realities faced by affected populations and are responsive to rapidly evolving conflict dynamics.

Towards a Risk-Based Prioritisation Framework

The table below summarises the four approaches and their pros and cons so that investors can consider which approach is most relevant to their context:

Approach	Short description	Key advantages	Key limitations
Controversy-based approach	Prioritises companies that have been linked to allegations, incidents or controversies identified through ESG data providers, media, NGO reports, litigation, regulatory actions or stakeholder complaints.	• Easy to implement using readily available ESG data. • Provides early warning signals on emerging concerns and reputational risks. • Helps identify companies that may require immediate engagement or escalation. • Often aligns with issues already attracting stakeholder attention.	• Reactive rather than preventive; harm may already have occurred. • Strongly dependent on external reporting and ESG provider methodologies. • Coverage of defence-specific risks (e.g. downstream due diligence, end-use risks, CAHRAs) can be inconsistent. • May create blind spots and fail to provide a comprehensive view of sector-wide risks. • Can overfocus attention on a limited number of highly visible companies.
Asset manager-level exposure	Prioritises individual companies representing the largest defence-related exposure across the investor's portfolio, combining financial materiality and involvement in defence activities.	• Strong alignment with portfolio materiality and stewardship priorities. • Easy to operationalise using holdings and exposure data. • Facilitates focused engagement with significant issuers. • Efficient use of limited HRDD resources.	• May overlook smaller companies involved in severe human rights or IHL risks. • Less sensitive to conflict-specific or context-specific risks. • Financial significance does not necessarily correlate with severity of adverse impacts.
Portfolio-level approach	Identifies portfolios, mandates or strategies that are structurally	• Scalable and systematic across large investment universes. • Identifies cumulative and systemic exposure	• Can generate a large universe of companies requiring assessment. • May miss indirect or value-chain exposures.

Approach	Short description	Key advantages	Key limitations
	exposed to defence-related risks, before conducting company-level assessments within those portfolios.	patterns. • Aligns HRDD with portfolio construction and investment processes. • Encourages a forward-looking and preventive approach. • Provides a broader view of sector exposure and peer comparison.	• Requires robust tools, data and internal expertise. • May be less responsive to rapidly evolving conflict situations.
CAHRA-focused approach	Prioritises companies linked to specific conflict-affected and high-risk areas, military operations, occupations or other situations presenting heightened human rights and IHL risks.	• Closely aligned with the OECD's severity-based prioritisation logic. • Focuses attention on situations where impacts may be most severe. • Helps build expertise on real-world defence and conflict-related risks. • Supports early engagement in situations of escalating concern. • Often aligns with stakeholder expectations regarding severe adverse impacts.	• Relies heavily on the quality and availability of external information. • Often reactive to already documented conflicts or allegations. • Provides a narrower perspective than portfolio-wide assessments. • May overlook other significant defence-related risks outside selected conflict contexts. • Can raise concerns about consistency or politicisation if selection criteria are not clearly defined.

No single methodology is likely to capture the full range of human rights and IHL risks associated with defence companies. Investors may therefore benefit from combining complementary approaches that consider financial exposure, portfolio characteristics, conflict-specific risks and emerging controversies. The appropriate balance will depend on an investor's resources, investment strategy, stewardship objectives and responsible investment philosophy. Ultimately, the goal is not to identify a single "right" methodology, but to develop a prioritisation framework that enables investors to focus their due diligence efforts where risks of adverse impacts are most significant and where they are best positioned to contribute to meaningful outcomes.

Once this prioritisation exercise has been completed, investors can move to the next stage of the process; conducting a more detailed assessment of the selected companies. Before examining a company's policies, governance structures or due diligence processes, it is essential to understand the context in which it operates. The next chapters address due diligence for priority review companies in more detail.

6. DUE DILIGENCE FOR PRIORITY REVIEW COMPANIES – PART A – CONTEXT

The previous chapter explored how to understand exposure and prioritise the identification of companies for more detailed review. There are multiple stages or elements which could be undertaken by an asset manager or asset owner when undertaking due diligence on a defence-related company. Prior to company due diligence, an investor may wish to establish the broad context relevant to the investment including export control regimes, company products and services, conflict-affected and high-risk areas, and relevant controversies and allegations. These elements are explored below.

Sections 6 and 7 focus on due diligence post-investment. Section 9 focuses on due diligence pre-investment. Section 10 focuses on company engagement. These elements have been drafted separately, but there is significant overlap between the sections in terms of the information investors may need to obtain and review. As such, elements of the appendices may be mixed and matched to support the specific use case of the investor. For example, appendix 7 has been created to provide starting point for pre-investment due diligence of companies. These questions may be suitable to support deeper company due diligence, but they do not allow for a deeper qualitative analysis as envisaged by the guidance below, or in Section 10 on company engagement.

Understanding the company context

Defence companies do not face identical risks, nor do they enjoy the same degree of visibility, leverage or control over the downstream use of their products and services. Their exposure to human rights and international humanitarian law (IHL) risks is influenced by a range of factors, including the export control regimes governing their activities, the nature of the products and services they provide, their position within the defence ecosystem, their exposure to conflict-affected and high-risk areas (CAHRAs), and any controversies or allegations linked to their operations.

These contextual elements help investors develop a more informed understanding of a company's inherent risk profile before evaluating the adequacy of its own policies and practices. They can also help identify where risks are most likely to arise, the extent to which a company may be expected to exercise oversight or leverage, and the types of safeguards that may reasonably be expected given its role and activities.

The following sections outline a number of contextual factors that investors may consider as part of a risk-based approach to company assessment.

Export control regimes

Arms sales and exports are prohibited, unless authorised by the competent authorities of the exporting States. Export control and arms transfer regimes constitute the primary mechanism through which States assess whether a proposed transaction may proceed.

Beyond traditional considerations relating to national security and foreign policy, these frameworks increasingly incorporate concerns related to international humanitarian law (IHL), human rights, regional stability and the risk of diversion.

International instruments, such as the Arms Trade Treaty (ATT), require exporting States to assess the potential consequences of a transfer before granting an export licence. States are expected to evaluate whether exported equipment could be used to commit or facilitate serious violations of IHL or international human rights law, and to deny authorisation where the relevant legal threshold is met.

For investors seeking to understand the human rights and IHL risks associated with defence companies, the existence of an export licence is therefore an important element of context. It indicates that the transaction has been subject to a governmental assessment and that the exporting State has considered the relevant factors through its own decision-making framework.

However, understanding that framework is equally important. While international agreements establish common principles, States retain significant discretion regarding how export controls are operationalised, how risks are assessed, what evidence is considered, and how different policy considerations are weighed in the final decision. As a result, export control regimes should not be viewed as homogeneous. They reflect distinct legal traditions, institutional arrangements, strategic priorities and geopolitical realities.

From an investor perspective, three dimensions are particularly relevant.

- First, it is important to understand how human rights and IHL considerations are integrated into the licensing process. Although many jurisdictions formally incorporate such considerations, the institutional mechanisms supporting the assessment may differ. The scope of interministerial consultation, the use of country risk analyses, the involvement of diplomatic, military or legal expertise, and the availability of post-export monitoring mechanisms can all influence how risks are evaluated in practice. Accordingly, understanding a company's home export control regime can provide valuable insight into the broader environment in which transfer-related risks are assessed and managed.
- Second, export control decisions should be understood within the broader geopolitical, economic and strategic context of the exporting State. Arms exports often sit at the intersection of foreign policy, defence cooperation, alliance commitment, industrial policy and national security objectives. These considerations do not negate the importance of human rights and IHL assessments but rather form part of the broader policy environment in which licencing decisions are made. Investors should therefore seek to understand not only the formal rules governing exports, but also the strategic context that may shape a State's approach to defence trade and international partnerships.

- Third, certain characteristics of specific export control systems may have implications for a company's overall exposure to risk. For example, some companies rely heavily on government-to-government transfer mechanisms, such as the United States' Foreign Military Sales (FMS) programme, in which the exporting State plays a particularly active role in the transaction. Other companies may be more dependent on commercial sales authorised through conventional licensing procedures. These distinctions can affect customer profiles, levels of governmental involvement, contractual structures, and ultimately the nature of the human rights and IHL risks to which a company may be exposed.

Importantly, the fact that a State has conducted an export assessment does not remove the relevance of corporate due diligence. As highlighted by the French National Contact Point for the OECD Guidelines in the Alsetex case¹¹¹, the existence of government controls and licencing procedures does not eliminate expectations that companies identify and address human rights impacts linked to their activities and business relationships. Rather, State assessments and corporate due diligence should be understood as complementary processes, operating at different levels.

As such, before assessing a company's policies, governance arrangements or individual transactions, it is essential to understand the export control regime within which the company operates. The degree of integration of human rights and IHL considerations, the broader strategic posture of the exporting State, and the specific characteristics of relevant transfer mechanisms can all materially influence a company's exposure to human rights and humanitarian risks. Without that contextual understanding, the analysis of the company itself risks being incomplete.

Please see *Appendix 9: Factors to bear in mind in assessing arms export regimes* for more detail. Appendix 7(D) provides a simple set of due diligence questions that may support investors in understanding this context.

Products and services

While export control regimes provide important context, they only offer a partial view of a company's exposure to human rights and IHL risks. Investors should also consider where a company sits within the defence value chain, the nature of the products and services it provides, and the degree of control it can reasonably exercise over their end-use. These factors can significantly influence both the company's inherent risk exposure and its ability to prevent, mitigate or respond to adverse impacts.

A useful starting point is to assess the company's position within the defence ecosystem as set forth in the Introduction to this chapter.

Prime contractors, system integrators and platform manufacturers typically maintain direct relationships with governments and military end-users, often playing a central role

¹¹¹¹ [Alsetex, Etienne Lacroix Group and Americans for Democracy and Human Rights in Bahrain \(ADHRB\)](#)

in the design, delivery and long-term support of defence capabilities. By contract, lower-tier suppliers may only provide components, materials or specialised technologies that are incorporated into larger systems. These distinctions matter because they shape both a company's proximity to potential adverse impacts and its leverage over customers, partners and downstream use. Companies operating closer to the end-user may have greater visibility over end-use and stronger opportunities to engage with customers, while suppliers further removed from the final deployment of a product may face more limited oversight and influence.

The nature of a company's products and services is equally important. Not all defence activities present the same level of inherent risks. Investors may wish to distinguish between platforms such as aircraft, naval vessels and armoured vehicles, weapons systems and munitions, components and subsystems, military support services and enabling technologies, such as surveillance systems, cyber capabilities or artificial intelligence applications. In general, companies involved in the production, integration or sustainment of weapon systems that can be directly employed in kinetic military operations are likely to face heightened exposure to IHL-related risks. Similarly, providers of operational support services, intelligence capabilities, or targeting enabling technologies, may be closely connected to military activities despite not manufacturing weapons themselves.

Particular attention may also be warranted where products fall within the scope of the ATT as conventional arms or key components thereof, where they can be directly used to kill or injure individuals, or where they support activities that raise heightened human rights or IHL concerns. Surveillance technologies, biometric systems, cyber-intelligence solutions and certain artificial intelligence may present significant IHL and human rights risks even when they have no direct combat function. Conversely, companies providing less sensitive products or services may face a different risk profile, although exposure can still arise depending on the customer, operating environment and intended use.

Investors should also consider whether a company has any involvement in weapons prohibited under international law or in other particular controversial weapon categories. Such involvement may alter the risk assessment significantly and may warrant separate consideration under an investor's responsible investment framework.

Ultimately, understanding a company's products, services and position within the ecosystem is not simply a matter of identifying what it produces, but a way of assessing how closely the company is connected to potential adverse impacts, the extent to which it can influence downstream use, and the practical limits of the due diligence measures it can implement. Two companies operating within the same national export control regime may present different risk profiles depending on their role in the defence value chain. Consequently, analysing a company's position within the ecosystem provides an essential complement to the assessment of the broader regulatory and geopolitical environment in which it operates.

Appendix 7(B) provides some initial due diligence questions for investors.

Revenue

Understanding the proportion of a company's defence-related revenue, the trend in revenue (i.e. growing or shrinking) and the importance of defence revenue or business activities is important context. For example, a company may generate a non-material percentage of revenue from defence but, due to the nature of its position with the national security picture, it is unlikely or unable to avoid or spin-out the defence segment (even if it reduced the companies legal, reputational and human rights risks). Appendix 7(A) provides some initial questions for investors to use.

Conflict-affected and high-risk areas

Understanding the export control framework applicable to a company and its position within the defence ecosystem provides essential context for assessing risk. The next step is to identify where the company operates and to whom its products and services are supplied. Exposure to conflict-affected and high-risk areas (CAHRAs) is particularly important, as these environments often present heightened risks of adverse human rights impacts, violations of international humanitarian law (IHL), diversion, misuse and governance failures.

For defence companies, exposure to CAHRAs may arise through exports to States engaged in armed conflict, the provision of products or services to military actors operating in conflict zones, support for coalition operations, or involvement in supply chains linked to regions affected by violence or instability. Such exposure does not necessarily imply that a company is contributing to adverse impacts. However, it increases the likelihood that products, services or technologies may be deployed in contexts where civilians face elevated risks and where compliance with IHL and human rights standards may come under particular scrutiny.

Investors should therefore seek to understand not only whether a company is exposed to conflict-affected and high-risk areas, but also the nature and extent of that exposure. This requires moving beyond a simple review of export destinations. The same country can present markedly different risks depending on the conflict dynamics, actors involved, the type of equipment supplied and the intended use of the products or services. Similarly, risks may differ significantly between a company supplying generic components and a company providing operationally critical capabilities that are likely to be deployed in active hostilities.

Particular attention may be warranted where products and services are supplied to parties involved in ongoing armed conflicts, where credible allegations of serious IHL or human rights violations have been documented, or where governance and accountability mechanisms are weak. In such circumstances, investors may wish to assess whether the company has considered the heightened risks associated with the operating environment and whether enhanced due diligence measures are implemented. Companies providing

products or services that are closely linked to combat operations, targeting functions or intelligence activities may face particularly acute exposure, given the potential connection between their activities and adverse humanitarian consequences.

Exposure must also be assessed dynamically. Risk profiles can change rapidly as conflicts evolve, political situations deteriorate, or new information emerges regarding the conduct of parties to a conflict. Markets that may have appeared relatively low risk at the outset of a commercial relationship can become significantly more challenging over time. For this reason, investors may wish to consider not only where a company currently operates, but also its capacity to monitor changing circumstances, reassess risks and adapt its commercial activities where appropriate.

Importantly, analysis of exposure to conflict-affected and high-risk areas should not be limited to direct legal or regulatory considerations. Companies operating in such environments may face heightened reputational risks, increased stakeholder scrutiny, litigation risks and allegations of involvement in adverse impacts, even where all relevant licenses and authorisations have been obtained. As a result, understanding a company's exposure to conflict-affected and high-risk areas is a critical complement to the assessment of export control regimes and product-related risks.

Ultimately, this analysis enables investors to identify where the most significant human rights and IHL risks are likely to arise and where enhanced scrutiny may be warranted. In doing so, it helps focus subsequent assessment of the company's due diligence processes, governance arrangements and risk management measures on the areas where they are likely to matter most.

Appendix 7(C) provides some initial due diligence questions for investors.

Controversies and External Allegations

In addition to understanding a company's operating environment, investors may wish to review controversies, allegations and public concerns linked to its activities, products or business relationships. Such information can provide useful insight into how human rights and IHL risks may manifest in practice and help identify areas that warrant further scrutiny during the due diligence process.

Relevant sources may include reports from civil society organisations, media investigations, litigation, parliamentary inquiries, OECD National Contact Point cases, UN mechanisms and ESG Data providers. Depending on the circumstances, controversies may related to arms transfers, customer relationships, allegations of product misuse, exports to conflict-affected areas, surveillance activities, corruption, or broader governance and compliance concerns.

However, controversies should be interpreted with caution and within broader context. The existence of an allegation does not necessarily demonstrate that a company has caused or contributed to an adverse impact, just as the absence of public controversies should not be interpreted as evidence that risks are adequately managed. Visibility often

depends on factors such as media attention, civil society capacity, the availability of information and geopolitical sensitivities, which may result in certain companies or conflicts receiving greater scrutiny than others.

Investors may therefore find it useful to consider controversies as one source of information, among many. Rather than serving as a standalone basis for assessment, controversies can help inform a broader understanding of company's exposure, highlight areas for engagement, and test whether the risks identified through the contextual analysis are reflected in real-world outcomes. Reviewing controversies alongside export control frameworks, product characteristics, value-chain positioning and exposure to conflict-affected and high-risk areas may provide a more balanced and comprehensive picture of a company's overall risk profile.

Appendix 7(F) provides an initial list of due diligence questions for investors.

Summary

While these factors do not, in themselves, determine whether a company is adequately managing human rights and IHL risks, they provide essential context for evaluating its performance. Indeed, two companies may have similar policies and due diligence processes yet face very different risk profiles depending on the export control framework in which they operate, the products and services they provide, their role within the defence value chain, and the environments in which their customers deploy those capabilities. Investors may therefore benefit from establishing this contextual understanding as a preliminary step, allowing subsequent analysis of company practices to be grounded in the realities of the operating environment rather than assessed in isolation.

7. DUE DILIGENCE FOR PRIORITY REVIEW COMPANIES – PART B – COMPANY POLICIES, PROCESSES & RISK MANAGEMENT

Building on the context, company level due diligence may further consider company human rights approaches, their approach to risk identification and prioritisation, their own due diligence in commercial and export decisions, product and technology safeguards, and their approach to transparency and engagement. This analysis should also enable a qualitative assessment of the company against the GRID Expectations.

Introduction

Investors take a broad range of approaches to investment due diligence depending on their individual needs. For example, pre-investment due diligence for a private equity investor, reviewing companies before allowing them to be part of specific funds will likely differ to ongoing due diligence for a public-company already in an index or actively management fund. This Guidance does not attempt to provide bespoke due-diligence for each use case but aims to provide frameworks that can be subsequently adapted by investors once a company has been *identified* for due diligence.

Users are reminded that the Guidance focuses on managing the financial, legal, reputational and human rights risks connected to the downstream use of products and services, and the relevant company operations (design, development, sale etc). As such, the Guidance below should complement wider due diligence considerations of environment, social, governance or sustainability factors an investor is interested in.

The steps below are realistically a starting point; investors may wish to explore companies in more detail where there are heightened or exceptional risks and further guidance will be considered to support such efforts.

Objectives of the Company Due Diligence

Once investors have identified priority companies and developed an understanding of the context in which they operate, the next step is to assess how those companies manage the human rights and IHL risks associated with their activities. This assessment should not be conducted in isolation from the contextual analysis described above. Rather, the company's due diligence framework should be evaluated considering its position within the defence ecosystem, the nature of its products and services, the export control environment in which it operates, and its exposure to conflict-affected and high-risk areas.

Importantly, investors should not necessarily expect the same safeguards, processes or level of visibility from all defence companies. A prime contractor exporting integrated weapons systems to conflict-affected regions may reasonably be expected to have more

sophisticated customer due diligence processes and end-use risk assessments than a lower-tier supplier providing generic components integrated into larger systems. Similarly, companies manufacturing surveillance technologies may require different controls than those producing conventional military platforms. Context should inform both the assessment of risks and the expectations placed on the company.

The objective is not to determine whether a company is simply “compliant” or “non-compliant”, but rather to assess whether its governance, policies and practices are proportionate to the risks it faces and whether it is taking reasonable steps to identify, prevent, mitigate and address potential adverse impacts linked to its products, services and business relationships.

The due diligence tools in Appendix 7 aim to translate investor *expectations* of companies into meaningful questions that can be asked (both through in-house research and to the company) in determining the company’s defence-context, the ability of the company to manage its risks and the nature of key concerns or controversies. These elements can be combined to inform the investor’s next steps, whether that is to invest, to not invest, to re-weight the company, to engage, escalate, ignore or potentially divest. The following sections provide further detail on the main questions that can be asked by investors and supplement the due diligence tools in Appendix 7.

The role of due diligence is not only to identify and help manage risks, but also to enable investors to make informed and consistent decisions regarding the activities, products, business relationships and behaviours they are willing to support through capital allocation.

Human rights commitment and governance

Please refer to the Chapter on Investor Expectations for more detail on what is expected of companies for both IHL due diligence and Heightened Human Rights Due Diligence. Appendix 7(G) and 7(H) both contain high level due diligence questions to establish a basic understanding of a company’s policies and processes relating to human rights.

Risk identification and prioritisation

Having established this overview, investors may then wish to assess how the company identifies and prioritises risks arising from its activities and relationships. In particular, they may wish to understand whether the company’s assessment extends beyond traditional compliance considerations and includes the potential impacts of its products and services on affected individuals and communities.

This may involve examining whether the company considers risks linked to customers, end-users and operating environments, including the potential misuse, diversion or unintended deployment of its products. For companies involved in sensitive technologies, such as surveillance systems, cyber capabilities, artificial intelligence or

intelligence support services, investors may also consider whether the company assesses risks associated with specific use cases and deployment scenarios.

A key consideration is whether risks are prioritised according to their potential severity for people rather than solely according to financial, legal or reputational consequences for the company. Companies operating in high-risk contexts should be able to demonstrate a clear understanding of the circumstances in which their products and services could contribute to adverse impacts and explain how those risks are incorporated into decision-making processes. Appendices 7(G) and 7(H) can support this assessment, but investors will likely need to generate a qualitative opinion on the company's approach to risk management.

Due diligence in Commercial and Export Decisions

For many defence companies, some of the most consequential decisions occur at the point of sale, contracting and customer engagement. Investors may therefore wish to assess the extent to which human rights and IHL considerations are integrated into commercial and export-related decision-making.

This does not mean expecting companies to replicate the role of governments or undertake parallel export licensing processes. Rather, the question is whether the company possesses internal mechanisms that allow it to identify heightened risks, seek additional information where appropriate, and escalate concerns to relevant decision-makers.

Factors that may be relevant include enhanced scrutiny of high-risk customers, destinations or technologies, procedures for reviewing potentially sensitive transactions, involvement of specialist functions in decision-making processes, and the company's ability to raise concerns internally when significant risks are identified. Depending on the company's role within the value chain, investors may also wish to understand the extent of its visibility over end-users and its ability to influence customer behaviour or contractual arrangements.

Appendix 7(E) provides a starting point for building this picture.

Product- and Technology-specific safeguards

Investors may also consider whether companies have implemented safeguards tailored to the specific characteristics of their products and technologies. While many risks arise from the context of use, certain technologies may present particularly foreseeable risks that can be addressed upstream during design and development.

Examples of safeguards may include safety-by-design or ethics-by-design approaches, product review procedures, restrictions on certain functionalities, internal guidance on acceptable and unacceptable uses, or dedicated oversight mechanisms for particularly sensitive technologies.

For companies developing surveillance capabilities, artificial intelligence applications, cyber tools or dual-use technologies, investors may wish to explore whether risk assessments consider not only the production of the technology but also its foreseeable deployment and operational use. Similarly, companies supplying products likely to be employed in kinetic military operations may be expected to demonstrate an understanding of how those products could be used in different operating environments and the safeguards implemented to manage associated risks.

Transparency, Stakeholder Engagement and Accountability

Finally, investors may assess how transparently the company communicates about its approach to managing human rights and IHL risks. Owing to commercial sensitivities, national security considerations and export control restrictions, complete transparency is rarely possible in the defence sector. Nevertheless, investors may reasonably expect companies to provide meaningful information regarding their governance structures, due diligence processes and risk management approach, as a minimum.

Investors may also consider the company's willingness to engage with stakeholders, including affected groups and their representants, experts and, where appropriate, civil society organisations and shareholders. Such engagement can provide important insights into emerging risks and help companies challenge internal assumptions about potential impacts.

In addition, investors may wish to examine whether mechanisms exist to enable concerns to be raised internally or externally, and whether the company has established processes for investigating and responding to allegations linked to its activities, products or business relationships.

8. INTEGRATION IN FUND DECISION MAKING

Once the investor has completed its due diligence, a key question becomes how the insights generated through it are meaningfully reflected in investment decision-making, rather than remaining confined to stand-alone analyses or engagement activities. The appropriate response will depend not only on the nature of the risks identified, but also on the investor's investment philosophy, responsible investment commitments, client expectations and objectives.

For some investors, due diligence findings (e.g. following a portfolio review) may lead to a reassessment of the types of defence activities, products or services they consider investable. While certain investors may already operate product-based restrictions relating to categories such as prohibited or controversial weapons, enhanced due diligence may also lead to the identification of additional activities considered incompatible with their investment policies or client mandates. Examples could include specific surveillance technologies, offensive cyber capabilities, technologies associated with severe human rights risks, or products that the investor considers present an unacceptably high risk of misuse or adverse impacts.

Similarly, some investors may conclude that exposure to certain customers, end-use scenarios or conflict situations exceeds their risk appetite, even where the activities remain lawful and authorised under applicable export control frameworks. In such cases, due diligence findings may inform the development of investment restrictions, eligibility criteria or enhanced approval processes for sensitive investments.

More commonly, however, due diligence findings are likely to inform a graduated set of responses reflecting both the severity of the risks identified and the investor's ability to influence outcomes. These responses may range from enhanced monitoring and engagement to investment restrictions, watchlist status or exclusion. In practice, investors may apply different escalatory responses, including:

- Enhanced monitoring;
- Internal watchlists;
- Targeted engagement;
- Voting actions;
- Restrictions on new investments;
- Suspension of purchases;
- Strategy-specific exclusions;
- Firm-wide exclusions.

Note on Exclusions - Importantly, exclusion should not necessarily be understood as the only or preferred outcome of due diligence. In many circumstances, continued investment coupled with active stewardship

may provide greater opportunities to encourage improved practices and strengthen risk management. Conversely, where severe risks remain unmanaged, where a company is unwilling to address identified shortcomings, or where the investor concludes that meaningful leverage is unlikely to exist, restrictions or exclusions may become appropriate tools for managing exposure and aligning portfolios with the investor's responsible investment commitments.

ESG assessments may also be integrated directly into investment analysis and portfolio construction, contributing to relative weighting decisions, determining eligibility within specific strategies, or supporting the application of selectivity rules. In some cases, weaker performance or unmanaged risks identified through due diligence may be reflected in lower ESG assessments, which could in turn affect a company's inclusion or weighting in certain portfolios. Conversely, evidence of more developed risk management practices may mitigate some concerns, even where exposure to high-risk activities remains.

Asset managers may find it useful to consider how qualitative findings from due diligence exercises can be translated into decision-relevant signals, alongside financial analysis and other ESG considerations.

One possible avenue, in addition to more commonly used levers such as engagement, escalation or exclusion, is to **integrate the conclusions of human rights due diligence into internal ESG assessment or rating tools**. Where asset managers already rely on ESG ratings to inform issuer selection or portfolio construction, incorporating due diligence insights into these tools may help ensure that human rights risks are taken into account in a more systematic and consistent manner.

In practice, human rights due diligence tends to generate a broad range of information, including greater understanding of companies' products and services, customer profiles, operating contexts, exposure to conflict-affected areas, governance arrangements and approaches to risk management. When assessed holistically, this information may offer a more nuanced view of how a company is exposed to, and seeks to manage, defence-related human rights risks. Integrating such insights into ESG tools can help reflect not only the presence of risks, but also differences in the quality and credibility of companies' policies, processes and practices.

Improved investment analysis - By adjusting ESG assessments to account for findings related to downstream due diligence, customer screening or product-related risks, asset managers may be better able to differentiate between companies facing similar external environments, but who demonstrate differing levels of preparedness, transparency or oversight. Over time, this may contribute to a better investment analysis which integrates human rights considerations.

Internal alignment - Embedding due diligence outcomes within ESG ratings can also support internal alignment. Once integrated, the analysis becomes part of the regular information set available to investment teams, rather than an additional layer of assessment considered only in specific instances. This may facilitate dialogue between ESG specialists and portfolio managers and support a shared understanding of why certain companies are viewed as presenting higher or lower levels of human rights risk.

Additive engagement - Importantly, integrating due diligence outcomes into ESG tools does not preclude the use of engagement. Rather, the two approaches can be mutually reinforcing. ESG assessments that highlight gaps or areas of concern may help prioritise engagement efforts and clarify expectations vis-à-vis issuers. Changes over time can also be monitored, allowing asset managers to assess whether engagement is contributing to improved practices or disclosures.

Weightings - Asset managers may apply environmental, social and governance (ESG) weightings within funds as part of portfolio construction and weighting. This may include the exclusion of poor performing companies, the inclusion of companies who meet ESG threshold scores, or the up/down weighting of companies within a fund based on their scores. Where investors apply ESG weightings, it is recommended that they consider the following approaches:

Integrating GRID Expectations – Investors have access to a wide range of proprietary and in-house ESG data sources from which to build ESG ratings of companies. This guidance will not attempt to set out model ESG criteria or scoring methodologies but recommends that internal ESG ratings at a minimum integrate sufficient metrics to understand how well companies are meeting the GRID Expectations set out previously.

Improving access to data – Investors should recognise the limitations of existing ESG data, supplement quantitative indicators with qualitative analysis where possible, and engage with issues and data providers to improve disclosure on human rights risks.

Setting progressive expectations – Where companies have progressively higher proportions of defence-related revenues, or have the greatest proximity to harms, investors could introduce progressively stricter ESG expectations, reflecting the increased inherent risks.

Clear methodologies – Investors should ensure that any ESG inclusion, exclusion or weighting criteria are clearly explainable to clients and companies. Defence related companies should be able to understand where and how they can improve on their ratings to enable inclusion in a fund or increased weighting within a fund.

Demonstrate processes - Finally, this form of integration may also assist managers in demonstrating how human rights considerations are taken into account in investment processes. While ESG ratings and internal tools are necessarily imperfect proxies for real-

world impacts, they can provide a degree of traceability and transparency regarding how assessments of risks to people inform investment decisions, which may be increasingly relevant in light of regulatory developments and stakeholder expectations.

Overall, integrating the results of human rights due diligence into investment tools such as ESG ratings can be seen as one possible way of strengthening the link between analysis and decision-making in the defence sector. When grounded in a contextual understanding of companies and used in combination with stewardship activities, this approach may help asset managers navigate complex risk environments in a more informed and structured manner.

9. PRE-INVESTMENT DUE DILIGENCE

*This section provides a framework for investors to use in their **pre-investment** due diligence to judge the risks associated with investment in a particular company across multiple dimensions of risk. Appendix 7 – Due Diligence Tools, provide an initial set of questions which investors can use to establish the company context and its ability to manage risks, informing how well placed it is to meet the GRID Expectations.*

Introduction

Investors will have a range of approaches to pre-investment due diligence. An asset owner considering the use of excuse rights for a private-market fund may only undertake a high-level review compared to the private market manager who is directly making the investment and requires a deep dive into all aspects of the company. Public market portfolio managers building funds based on ESG exclusion and inclusion criteria may focus on a combination of revenue, products and services, controversies and wider ESG factors.

Appendix 7 ‘Due Diligence Tools’ provides a simple framework for pre-investment due diligence designed to support several use cases. The framework is designed to build on the GRID Expectations and create meaningful enquiries that can determine the company’s defence exposure and risk context and its approach to managing risks. The output is designed to feed into the overall investment decision-making process.

This framework focuses on understanding the following for a company:

- A. Defence-related revenues
- B. Defence-related products and services
- C. Geographic footprint and exposure to conflict affected and high-risk areas
- D. Applicable regulatory and legal frameworks
- E. Customers, end-users and business relationships
- F. Exposure to controversies
- G. Company policies relating to GRID Expectations (avoid legal complicity, respect for human rights, anti-bribery and corruption, political advocacy and lobbying)
- H. Company processes and management relating to GRID Expectations (legal complicity risk management, human rights due diligence, anti-bribery and corruption management systems, contractual controls, mitigating processes, political advocacy and lobbying controls, expertise and governance)

The framework enables investors to select to have a high-level qualitative understanding of the company and to score the company in various ways (e.g. ‘very high inherent risk’ for products [red], ‘very low geographic risk’ [green], full/poor alignment with GRID Expectations etc). Based on the output of initial due diligence, an investor could create a summary assessment using the aspects it considers most relevant, as set out in the example table below:

Indicator	Rating	Notes
Revenue Exposure	● High	Approximately 45% of revenue derived from flagged activities
Position in Value Chain	● Medium	Supplies components; not a direct end-product manufacturer
Geographic Risk	● Low Risk	Only operating in home state and not exporting to or working with other nations
Controversy History	● Low Risk	No major incidents in past five years; proactive disclosure
Policy and Processes	● Medium	Meets minimum standards; enhanced monitoring recommended
Overall Risk Rating	● Medium	Red revenue flag offset by limited operational proximity to potential harm and absence of controversies. Potential to improve policies and processes to meet expectations.

Understanding outputs

Based on the outputs of the pre-investment assessment, investors can develop a qualitative view of the company to inform decisions on whether to invest, avoid investment, conduct further due diligence or engage.

A high-risk or red indicator across one or more dimensions of the framework is unlikely to automatically render a company uninvestible, but each investor must set their own approach. Outputs of an assessment should be read holistically rather than in isolation. For example, a company may show a red rating on revenue exposure — indicating significant financial dependence on high-risk activities — yet this can be substantially offset by the presence of robust internal controls, strong governance mechanisms, meaningful distance from the most harmful points of the value chain, and a demonstrated track record of effectively managing controversies when they arise.

Next steps

Based on the outputs of the initial framework, investors can make decisions concerning green-lighting investments, conducting deeper due diligence based on desk-based research, engaging with the company, and avoiding exposure.

Where deeper due diligence is required, sections 6 and 7 (post-investment due diligence) and 11 (engagement) should be useful for investors. However, investors should be aware that there may be severe limitations on the availability or willingness of companies to provide information and therefore investors will need to establish boundaries concerning inabilities to conduct deeper due diligence.

10. NAVIGATING CONTROVERSIES (INCLUDING RESPONSIBLE DIVESTMENT)

This section addresses how an investor can assess and respond to controversies. It should be read together with the Engagement section, which sets out how managers should structure and escalate dialogue with companies, and the Due Diligence sections, which provide the framework for understanding a company's risk profile and the quality of its risk management systems. Controversy handling is not a standalone exercise; it is most effective when grounded in an understanding of the company's context and supported by meaningful engagement.

Introduction

Controversy monitoring and management is a common investor activity. It is also frequently a key tool to identify human rights risks and impacts relating to investments and is therefore likely already part of an investors implementation of the UN Guiding Principles on Business and Human Rights¹².

To navigate legal, reputational, financial and human rights risks for defence related investments, investors should therefore implement processes to identify and address relevant controversies.

***Note** – This section has been drafted to be quite high-level and cut across different types of controversy. Readers are encouraged to consider what specific guidance would be desired in terms of handling very serious controversies, such as allegations of company complicity in International Crimes, or on how to identify such controversies.*

Supporting tools

Investors may choose to place different emphasis on types of controversies (for example, an asset owner may focus on emergent controversies relating to alleged breaches of international norms, while an active public equities manager may also consider wider risks including reputational issues).

The Investor Initiative on Human Rights Data (II-HRD) has produced [Guidance for ESG data providers on assessing company non-compliance with, and breaches of, international human rights norms](#). While directed primarily at ESG Providers, the Principles set out in the guidance are also useful for investors trying to identify and address norms-based controversies.

¹² It is noted that some investors may delegate their controversy process to third parties e.g. managers.

Understanding types of controversies

The starting point for any controversy assessment is to understand the nature and basis of the concern. Not all controversies are equivalent, and investors should distinguish between reputational exposure and normative breach. A company may face significant media or NGO attention without having caused, contributed to, or been directly linked to a genuine violation of international norms. Conversely, a company may be involved in serious breaches of IHL or IHRL law that have not yet attracted significant public attention.

Investors are therefore recommended to distinguish between the following categories of concern:

- **Allegations of IHL breaches or complicity**, including credible claims that the company's products, services or business relationships have been used in the commission of war crimes, crimes against humanity or genocide, or have contributed to unlawful attacks on civilians or civilian infrastructure. Generally, these claims will warrant the most serious and urgent response.
- **Allegations of IHRL breaches**, which may be within its own workforce or supply chain and may not relate to the end-use of the product.
- **Export control and sanctions violations**, including credible evidence of the supply of products or services in contravention of applicable licensing requirements, arms embargoes or sanctions regimes.
- **Bribery, corruption and improper conduct**, including OECD National Contact Point complaints, criminal investigations or civil proceedings relating to the company's business practices.
- **Product misuse and diversion**, including situations where the company's products or services have been used in ways inconsistent with stated end-use assurances, or have been transferred to unauthorised third parties, which may have occurred with or without the company's knowledge. It may also be the case that a company that did not previously engage in business involving prohibited or controversial weapons later develops its business in this area.
- **Reputational controversies**, including significant media coverage, civil society campaigns or investor pressure that may not reflect a direct normative breach but nonetheless create material legal, reputational and financial risks.

Assessing severity

The following factors may be relevant in considering the severity of a controversy:

- Is the controversy based on an allegation or finding of breach/wrongdoing?
- What is the evidence for a controversy which is alleged rather than proven – does it come from a single source, or multiple sources? What is the credibility of the sources?

- Is the controversy seemingly more serious only because of the high profile of the company or the conflict situation in question? Assessments may skew against companies with already high public profiles, as well as companies operating in high-visibility conflicts.
- What is the actual, alleged or potential harm and how serious is it?
- Where in the value chain does the company sit – could it be said to have caused or contributed to the harm, or is it directly linked?
- Are there indicators that this event reveals a systemic failing in the company's governance and risk management framework, or a one-off?

Further analysis

Once the severity, veracity and company connection to a controversy has been established, investors are recommended to also establish:

- The effectiveness of prevention, mitigation and remediation measures which the company has put in place;
- The quality of the company's due diligence processes;
- The likelihood of future adverse impacts (informed by the ongoing / repeat nature of the controversy/events, as well as the ability of the company to avoid or mitigate risks); and
- The investor's own ability to exercise leverage and influence outcomes.

Investor responses

Controversies require careful analysis before any action is taken, to avoid decisions that are driven by external pressure rather than by a genuine assessment of normative risk. Once an investor has fully understood the picture, a range of responses is available, with the following broadly sitting on a sliding scale of seriousness, though not all of these will be possible in all cases, and some will be more appropriate for different types of holdings and investors:

1. **Monitoring**, where the concern is at an early stage, information is incomplete, or the company has not yet had a reasonable opportunity to respond.
2. **Targeted engagement**, where the investor has sufficient leverage to raise concerns directly with the company, request additional information or disclosures, and set expectations for remediation or improvement within a defined timeframe.
3. **Collaborative engagement**, where the concern is shared by other investors and a coordinated approach may provide greater leverage or credibility.
4. **Voting and public escalation**, where bilateral engagement has not produced sufficient progress and the investor has the tools and mandate to escalate through shareholder resolutions, public statements or voting actions. In a private markets context, this may mean using contractual rights or governance tools.

5. **Portfolio restriction or watchlist status**, where the concern is sufficiently serious to warrant limiting new investment or placing the company under heightened monitoring pending further information.
6. **Divestment**, where appropriate (see below).

Controversy related divestment

Divestment may not be possible in all cases – in illiquid investments, disposal may be impractical or seriously detrimental to investor interests. It should also not be the default in many cases. As noted in the Exclusionary Screening section, divesting from companies connected to certain conflicts purely on the basis of that connection precludes positive engagement and could lead to the exclusion of companies that have not caused, contributed to or been directly linked to adverse human rights impacts or IHL breaches. Divestment by investors and managers committed to responsible investment principles can also reduce overall oversight and engagement with the company.

The manager should consider carefully whether the continued holding of the company is consistent with the commitments it has made to investors and the defence investment positions of those investors. Managers whose funds have more than minimal exposure to defence investments should ensure that their arrangements with investors provide sufficient flexibility to resolve controversies in an appropriate way. This may include an explicit acknowledgement that divestment will not be an automatic requirement and a period of engagement with the aim of resolution will be permitted.

While it is recognised that some investment mandates stipulate blanket divestments from companies connected to certain conflicts or issues, the Guidance encourages investors to focus on their responsibilities under international business and human rights norms. They are encouraged to prioritise understanding where companies are causing, contributing or are directly linked to adverse impacts, how adequately the company has responded, the likelihood of future adverse impacts, and the current and future human rights risks of remaining invested in that company. Further, in line with those norms, investors should utilise their own leverage to address those adverse impacts, rather than automatically exiting the relationship. Where investors are unable to build and exercise sufficient leverage to prevent or mitigate those adverse impacts, divestment may be an appropriate response (noting the limitations set out above). However, any potential adverse human rights impacts of divestment should also be assessed to avoid creating further problems and to ensure responsible divestment.

11. ENGAGEMENT

This section addresses post-investment engagement between asset managers and portfolio companies. It builds on the section on pre-investment due diligence by focusing on elements which may remain of concern to the asset manager during the holding period.

Company Engagement

Engagement is a core tool for investors to test whether defence-related companies have governance, systems and decision-making processes commensurate with the severity and complexity of the risks identified through pre-investment due diligence. It complements, but does not replace, due diligence. DD tells investors what the risks are – while engagement tests how the company manages them in practice, and what evidence it can provide.

Engagement is particularly important in the defence sector because the most severe risks to people typically arise downstream – through the use, misuse, diversion, servicing or integration of products and services into military operations and security contexts. This differs from many other high-risk sectors, where harms are more commonly concentrated upstream (e.g. labour conditions in supply chains). Dialogue can help investors understand how downstream risks are governed, give companies the opportunity to explain context and legitimate constraints, and identify gaps where public disclosure does not fully reflect internal practice.

Engagement is generally most effective when framed around financial materiality — proximity to conflict, military operations or security forces in CAHRA can give rise to heightened legal and regulatory exposure, reputational and commercial risk, and longer-term impacts on resilience, valuation and access to capital. Framing engagement in these terms locates human rights considerations within core risk management and investment analysis, rather than treating them as peripheral or purely ethical concerns.

Scope, proportionality and constraints

Engagement expectations should be applied on a risk-based and proportionate basis, recognising that investors' leverage varies by asset class, ownership level, mandate and investment approach. Investors should also recognise legitimate security, legal and contractual constraints on disclosure in the defence sector, and adapt evidence requests accordingly (including through confidential engagement where appropriate). These constraints do not remove the relevance of due diligence and governance questions; rather, they shape what can reasonably be evidenced and how progress can be demonstrated.

Using engagement questions to assess robustness and transparency

Rather than prescribing specific operational outcomes, engagement is often firstly conducted through targeted, risk-based questions designed to understand the robustness of company systems and the quality of governance and oversight. Questions should be framed to support dialogue and clarification, including by distinguishing between verified information and allegations or external reporting, and by giving companies a reasonable opportunity to provide additional context.

Tips

- *Ask for practice, not just policy: frame questions in a way that asks for outcomes and examples of how policies are applied in practice.*
- *Avoid cherry-picked examples by grounding questions in specific contexts (a named conflict/region, a defined timeframe, or a defined product line/customer type).*

Example engagement questions tailored to defence-related companies

The engagement questions follow the same structure as Pre-Investment Due Diligence. Rather than repeat the DD questions, the prompts below focus on what dialogue is uniquely placed to test: evidence, judgement, examples, and disclosability. Investors are encouraged to draw the underlying substantive questions directly from the corresponding DD sub-section, and to use the prompts below to sharpen the engagement lens.

Prompts should be adapted based on business model, product category, customer base and risk exposure, and grounded in specific contexts (a named conflict/region, a defined timeframe, or a defined product line/customer type) to avoid cherry-picked responses.

See Appendix 8: Engagement questions for Companies for a full list of suggested questions

Engagement as an ongoing and proportionate process

Engagement on defence-related and CAHRA-linked risks should be understood as an ongoing and proportionate process, rather than a one-off interaction. Where concerns persist – for example due to limited evidence of progress over multiple engagements, persistent opacity not justified by genuine constraints, or inability to mitigate severe risks – investors may consider escalation through continued dialogue, collaborative engagement, voting, or capital allocation decisions, consistent with fiduciary duties and client mandates.

Escalation

Where engagement does not provide sufficient comfort that risks are being managed in line with international norms and this Guidance, investors may escalate progressively and proportionately. For example:

1. Requesting clearer evidence and time-bound actions.
2. Pursuing collaborative engagement.
3. Using voting and public escalation tools where appropriate.
4. Considering capital allocation decisions where risk remains unmanaged or transparency is persistently insufficient.

Engaging with the defence ecosystem: dialogue with public authorities and industry bodies

In the defence sector, human rights due diligence and ESG integration cannot be approached solely through bilateral relationships with investee companies. The structure of the sector, and particularly the central role played by public authorities, means that investors may also need to engage with the broader defence ecosystem to develop informed, credible and context-aware approaches.

Why ecosystem engagement matters

Defence companies operate within legal and regulatory frameworks that are approved, shaped and overseen by governments. Public authorities typically determine which exports are authorised, which programmes are funded, and which strategic priorities govern industrial development. These decisions directly shape the conduct of defence companies and the risks to which investors are exposed. In a sector characterized by strong public oversight and complex geopolitical constraints, building channels of dialogue with competent authorities and industry bodies may therefore constitute an important, albeit often overlooked, component of investor human rights due diligence.

Engagement with procurement and export authorities

In most defence-producing countries, one or more central government bodies will generally be responsible for procurement, industrial policy and export licensing. Cooperation may involve working groups in which both industry and these public authorities participate. Where governments have established dedicated forums for dialogue between investors and the defence ecosystem, participation can support mutual understanding while providing a channel through which responsible investment expectations can be communicated to relevant decision-makers.

Engagement with industry bodies

Industry associations representing defence companies act as intermediaries between public authorities, industrial actors and external stakeholders. Through thematic working

groups and collective initiatives, they may contribute to the diffusion of best practices on governance, compliance and risk management. Engagement with these platforms can complement company-level due diligence by offering sector-wide insights and facilitating structured dialogue at scale.

Engagement with national human rights institutions and oversight bodies

National human rights institutions, parliamentary oversight committees and independent bodies with mandates relating to arms transfers can provide valuable inputs for investors. These institutions may publish reports identifying weaknesses in arms control implementation or put forward recommendations to governments and companies. Credible reports from such bodies can help inform engagement priorities.

Practical Guidance

Investor engagement with defence-related companies can be challenging for a variety of reasons. Where investors cannot achieve meaningful engagement outcomes through company engagement, where the systems do not encourage companies to meet the GRID expectations, or where accountability mechanisms are insufficient to hold companies accountable and/or mitigate defence-related risks, investors should consider engagement with government and key stakeholders to address gaps and positively influence the ‘rules of the game’.

In some situations, even well-designed national level legislation may not be sufficient to address the issues identified by investors. In this scenario, investors are recommended to explore engagement relating to international law, treaties and agreements. Investors have significant experience of engagement at this level, for example on issues such as climate change and nature loss, and there is an opportunity to take the learnings from those engagements and apply them to the defence context.

Example – Autonomous Weapons Systems

Some investors may have significant concerns about lethal autonomous weapons systems (LAWS). Engaging with defence-tech companies on the issue of LAWS may result in positive outcomes with companies. But investors should recognise the cumulative market and political pressures which may encourage companies to rapidly pursue the creation of LAWS, and how that may hamper any engagement efforts. In this case, engagement at both national and international level may be needed to explore appropriate controls, such as an international treaty regulating autonomous weapon systems.

See Appendix 2 for a case study on France’s approach to industry engagement.

12. COMMUNICATING TO CLIENTS AND STAKEHOLDERS

Key takeaways

Investor communication may:

- *Make the policy usable by explaining how defence-related exposure is defined, how dual-use activities are treated, and what may lead to engagement, escalation, portfolio restrictions or exit¹³;*
- *Be proportionate to the investor's role, mandate, asset class, resources and level of control over investment decisions, recognising that asset managers, asset owners, passive investors, private market investors and investors using external managers will apply the principles differently;*
- *Support informed dialogue with clients, beneficiaries and relevant stakeholders, including by explaining how feedback is considered, how competing preferences are handled, and how policy updates are made;*
- *Balance transparency with confidentiality by providing meaningful reporting on exposure, data sources, stewardship themes, controversy response and policy changes, while recognising legal, security and commercial limits on disclosure.*

1. Explain the scope and decision process

Investor communication on responsible defence investing should go beyond generic responsible investment policy disclosures. Investor communication should allow clients and other stakeholders to understand how the investor defines defence-related exposure, including products, services, customers and enabling technologies. They should also understand how companies or activities with both civilian and defence uses are treated, which decisions apply across the organisation, and which depend on a specific mandate, product or client instruction.

Communication should also aim to explain within reasonable boundaries how difficult decisions are made. This includes who is involved, what evidence is used, how controversies are assessed, and what may lead to engagement, escalation, portfolio restrictions or exit. Defence-related activities raise different considerations depending on the product, customer, end use, jurisdiction and mandate, so investors should explain the scope of their responsible defence policy in practical terms. This includes how they classify various defence products and activities, and where revenue thresholds, ownership links, subsidiaries, joint ventures, supply chain exposure or external data sources are relevant, these should also be explained clearly.

¹³ Final version may include examples or links to examples of strong policies

Investors relying on external data providers, ratings, screening tools or index methodologies should acknowledge that definitions, revenue classifications and controversy assessments may differ across providers.

2. Apply expectations proportionately

Communication should be proportionate to the investor's role, mandate, size, resources, asset class exposure and level of control over investment decisions. A large active manager, passive manager, small asset owner, pooled fund provider, external manager platform or investor allocating through third-party funds may apply the same principles through different mechanisms.

Asset managers should explain which exclusions or restrictions apply across the firm, which are strategy-specific, and where client preferences can be reflected through mandate design. Asset owners should connect defence-related investment decisions to fiduciary duty, investment beliefs, responsible investment policy and beneficiary expectations. Where asset owners invest through external managers, communication should explain how responsible defence expectations are reflected in manager selection, mandate design, monitoring, reporting requests and escalation with managers.

3. Explain the tools available to the investor

Investors should explain which tools are available in the relevant product or mandate, and how they are used in practice.

Stewardship communication should also be realistic about investor influence. Investors can set expectations of defence companies on governance, compliance, human rights due diligence, lobbying transparency, anti-bribery and corruption controls, cybersecurity, governance of AI-enabled and autonomous systems, and controls over product design, sales, end use and misuse risks. They can also ask companies to strengthen board oversight, improve disclosure and provide more robust escalation processes for high-risk contracts or technologies. Some decisions sit primarily with governments, regulators and procurement authorities. Communication should recognise those limits while making clear what investors still expect from issuers and external managers.

If these expectations are emerging or evolving, investors may consider acknowledging the limitations of existing approaches, or be transparent on where the discussions are evolving, and how they mitigate the relevant risks.

4. Use communication to inform policy development

Investors should use appropriate channels for clients, beneficiaries and relevant stakeholders to provide input into how responsible defence policies evolve. These channels may include client consultations, mandate reviews, advisory forums, stewardship briefings, trustee discussions, beneficiary surveys, member forums or stakeholder panels, depending on the investor and mandate. They can also support information exchange, including sharing research, identifying emerging concerns and

clarifying where clients need further analysis to understand exposure or policy implications.

Relevant stakeholders will vary by investor and mandate. They may include clients, beneficiaries, trustees, consultants, civil-society experts, affected-stakeholder representatives, regulators, policymakers or other parties with relevant expertise. Their input should inform policy review and risk understanding, while final decisions remain subject to fiduciary duties, legal requirements, investment objectives and governance processes. Investors should explain how feedback is considered, who reviews it, and how it may influence policy updates, mandate design, stewardship priorities or reporting. They should also be clear that preferences may differ across clients and beneficiaries.

5. Prepare for controversies and concern-raising

Investors should be clear on how they would respond to controversies that may arise from defence investments. Clients and stakeholders should understand what happens when credible allegations arise. Communication should explain the types of evidence considered, how allegations are distinguished from findings, and what may lead to continued monitoring, engagement, voting action, watchlist status, restrictions or exit.

Where relevant, investors should also explain how clients, employees or other stakeholders can raise concerns about defence-related holdings, mandate implementation or possible inconsistencies with the stated policy, including through existing complaints, whistleblowing, ethics or client-service channels.

6. Balance transparency with confidentiality

Given the sensitivity of the sector, investors should define what can and cannot be disclosed. Detailed information on government contracts, customer relationships, security arrangements, export licences, supply chains or engagement content may be confidential or security-sensitive. This should not, however, prevent useful reporting. Investors can provide aggregate information on portfolio exposure, engagement themes, companies reviewed, issues escalated, policy changes requested and progress updates where disclosure is possible. Where information cannot be shared, the reason should be stated clearly.

Public communication should focus on the investor's responsible defence policy, including definitions, exclusions, decision governance, escalation criteria, stewardship priorities, exposure reporting and the policy review process. Public reporting should avoid broad claims about contribution to peace, security or human-rights outcomes unless those claims can be supported. More credible communication will usually focus on risk management, mandate alignment, investment rationale, stewardship expectations and explanation of how decisions are made and reviewed. Investors should also prepare for media and public scrutiny by ensuring that external messaging is consistent with policy, portfolio practice and client reporting.

Private client communication can provide more detailed mandate-level exposure analysis, revenue-band reporting, discussion of contentious holdings, case studies, controversy updates and explanation of changes in portfolio positioning. For pooled funds, investors should be clear about the limits of client customisation. For segregated mandates, they should explain how client-specific restrictions, thresholds or reporting requirements are implemented and monitored. For asset owners using external managers, private reporting can also cover manager alignment, exceptions, data gaps and follow-up actions.

7. Align internal messaging and review the policy over time

Internal communication is also important in maintaining overall transparency and consistency on defence investments and how this is relayed to internal and external parties. Client-facing teams, portfolio managers, stewardship specialists, responsible investment teams, data teams, public affairs teams and risk functions should work from a shared account of the responsible defence policy. Internal guidance should cover definitions, data sources, permitted and excluded exposures, treatment of dual-use activities, escalation triggers, approved reporting language and responses to common client questions. Consistency may also require regular training and information exchange between the relevant teams.

Where investors engage with regulators, policymakers or industry bodies, relevant internal teams should coordinate positions so that policy engagement, stewardship messaging and client communication remain consistent.

Responsible defence policies will require periodic review. The boundaries of the sector are changing as defence increasingly intersects with cyber, AI, autonomous systems, data infrastructure, satellites, semiconductors and other enabling technologies. Communication should explain how the investor monitors these changes and when the policy, classification criteria or reporting will be updated. Clients and stakeholders should understand that responsible defence investing requires documented responsibilities, evidence standards, review points and escalation routes for applying policy to a sensitive and evolving investment area.

-----APPENDICES BELOW-----

Appendix 1: Definitions

Note – See the Expectations Chapter for a larger list of definitions and explanations of key concepts.

Conflict affected high risk area (CAHRA) – There is no universally agreed definition of what constitutes a CAHRA (and also no globally agreed list of CAHRAs). The definition provided in Regulation 2017/821 of the EU, concerning supply chain due diligence obligations for certain materials from conflict-affected and high-risk areas is as follows: *‘Conflict-affected and high-risk areas’ means areas in a state of armed conflict or fragile post-conflict as well as areas witnessing weak or non-existent governance and security, such as failed states, and widespread and systematic violations of international law, including human rights abuses*¹⁴.

Controversial weapons – Definitions of controversial weapons may vary by jurisdiction. For the purposes of this Guidance, it includes weapons that are either absolutely prohibited under customary international humanitarian law or specific IHL treaties, or whose use is regulated or restricted due to their indiscriminate or disproportionate effects. These include biological weapons, chemical weapons, cluster munitions, anti-personnel landmines, nuclear weapons (as addressed by the Treaty on the Prohibition of Nuclear Weapons), incendiary weapons, non-detectable fragment weapons, expanding bullets, exploding bullets, and blinding laser weapons. Autonomous weapons systems are included as an emerging category under active international discussion.

Dual-use – Dual-use items are goods, software and technology that can be used for both civilian and military applications. Trade in dual-use goods may be regulated at a national level as part of the export licensing and control framework, often by reference to a fixed list of dual-use items. According to the UN Working Group on Business and Human Rights, the fact of falling within or outside dual-use regulation is not determinative in an assessment of actual or potential human rights impacts. Commercial items may still be used in a manner contrary to international law, and their export to a given context may also be prohibited by international law. In these circumstances, while the product itself may not entail inherent risks to human rights, the end-use context may entail a risk of severe human rights impacts.

Ethical investing – An investment approach guided by moral or values-based principles, which may vary significantly depending on the ethical framework of the investor. The RBC standards can be seen as operationalising a baseline of ethical expectations grounded in internationally recognised human rights norms, but ethical investing encompasses a broader range of approaches. It is particularly varied in faith-based investing contexts. This Guidance is intended to be useful for ethical investors without taking an ethical

¹⁴ [Regulation - 2017/821 - EN - EUR-Lex](#)

position on defence activities or investments beyond those set out in the RBC standards and GRID Expectations.

Human rights due diligence (HRDD) – Human rights due diligence is the ongoing process by which a company identifies, prevents, mitigates, and accounts for how it impacts people’s human rights through its own activities and its business relationships. It is a continuous risk-management process focused on risks to people, not risk to the organisation. HRDD is anchored in the UNGPs, meaning that all companies, regardless of size, sector or location, are expected to identify, prevent and mitigate human rights risks and impact, track the effectiveness of their actions and communicate their efforts and progress.

Heightened human rights due diligence (HHRDD) – The UNGPs envisioned HRDD processes being proportionate to the risk, with heightened risk contexts resulting in ‘heightened human rights due diligence’. Conflict Affected and High-Risk Areas (CAHRAs) generate elevated risks of human rights abuses. Where companies are operating in or connected to CAHRAs they should therefore be conducting HHRDD. HHRDD is not just ‘more due diligence’. “Heightened human rights due diligence strengthens the understanding of the context where businesses operate and ensures that their activities do not contribute to violence by identifying flash points, potential triggers or the forces that are driving the conflict”.¹⁵

Impact investing - An investment approach that seeks to generate measurable positive social or environmental outcomes alongside financial returns. There is ongoing debate as to which investments qualify as impact investments. Whether any defence-related company or activity can be classified as an impact investment is not addressed by this Guidance.

International humanitarian law (IHL) - International humanitarian law (IHL) is also known as ‘the law of armed conflict’ or ‘the law of war’. Its fundamental premise is that even in times of armed conflict human dignity must be respected and protected, and the means and methods of warfare regulated. Rules reflecting these principles can be found throughout history in most if not all cultures. The law of armed conflict is based on customs and traditions and our experience of armed conflict throughout the ages. A good example is the universal ban on poisoning as a form of warfare, which dates to ancient times when, for example, the military on both sides would issue orders not to poison wells, as much for their benefit as for that of the civilian population – they might need the water one day.

International human rights law (IHRL) lays down obligations which States are bound to respect. By becoming parties to international treaties, States assume obligations and duties under international law to respect, to protect and to fulfil human rights. The

¹⁵ [Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide | United Nations Development Programme](#)

obligation to respect means that States must refrain from interfering with or curtailing the enjoyment of human rights. The obligation to protect requires States to protect individuals and groups against human rights abuses. The obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights¹⁶.

Responsible Business Conduct (RBC) – Responsible business conduct is the expectation that enterprises prevent, mitigate and remediate adverse impacts on people, the environment and society associated with their activities and business relationships, and contribute to sustainable development, through risk-based due diligence and responsible governance. This expectation is reflected in the OECD Guidelines and is consistent with the UN Guiding Principles on Business and Human Rights, the ILO MNE Declaration, and other international instruments.

Sustainable investing - At international level, there is no single universally agreed definition of what constitutes a sustainable investment. While sometimes definitions focus only on environmental aspects of sustainability, many will alternatively or additionally take into account social factors. The concept has been shaped primarily through regional or national regulatory initiatives, including sustainable finance frameworks, taxonomies and disclosure regimes, which may vary significantly in their scope, criteria and underlying assumptions. The interpretation of sustainability therefore remains contextual and jurisdiction-dependent. This Guidance does not seek to classify defence-related activities or companies as sustainable or non-sustainable.

¹⁶ [International Human Rights Law | OHCHR](#)

Appendix 2: Case Studies

Investor Example - LBP AM's approach to integrating company-level human rights due diligence into investment analysis

LBP AM conducted a study on major European defence companies, designed as a deep-dive exercise aimed at strengthening the understanding of defence-related human rights risks and at exploring how such insights could be integrated into existing investment processes. Rather than seeking to produce a standalone or prescriptive framework, the objective was to develop an approach that could complement existing ESG analysis, while taking into account the specificities of the defence sector.

Building a contextual understanding of each company

A first step consisted in developing a detailed and contextual understanding of each company analysed, going beyond high-level sector classifications or revenue thresholds. This involved gathering information on the nature of the company's activities, its position in the defence value chain and its exposure to sensitive products, technologies and services.

Particular attention was paid to identifying key products and capabilities, including weapon systems, platforms, subsystems, and enabling technologies such as surveillance, cybersecurity or artificial intelligence. The analysis also considered the role of each company within major European or international defence programmes, as well as its reliance on export markets and long-term service or support contracts, which can extend exposure to risk over time.

Understanding the customer base and operating context was another central element. The study sought to identify the types of customers served, the visibility over end-users and end-use, and exposure to conflict-affected or high-risk areas. This contextual analysis was essential to assess where severe human rights risks might plausibly arise, independently of how companies describe their own risk profiles.

Finally, the applicable regulatory environment was examined, including export control regimes and relevant national or European legislation. While recognizing the role of States in authorizing exports, this element was used to frame the analysis of corporate responsibility under international standards.

Focusing on how companies identify and manage risks

Building on this contextual groundwork, the study then explored how companies approached human rights risk management in practice. The analysis was structured around three broad and interrelated areas, chosen to reflect the logic of international standards, while remaining adaptable to investor use.

The first area concerned human rights commitments and governance. This included an assessment of the existence and scope of public commitments, alignment with international standards, clarity regarding downstream activities, and the extent to which oversight and accountability were embedded within governance structures. The presence or absence of dedicated resources, internal expertise and training were also considered as indicators of organization capacity.

The second area focused on risk identification and prioritisation. The study examined whether companies identified risks beyond their own workforce and supply chains, and whether they explicitly considered risks related to customers, end-use, conflict situations or sensitive technologies. Attention was paid to the degree of granularity, transparency and prioritisation in risk mapping, especially where risks were severe but less visible.

The third area assessed the implementation of due diligence and the level of residual risk. This included reviewing how human rights considerations were integrated into sales, contracting, export and product development processes, whether enhanced scrutiny was applied in high-risk situations, and how companies described their ability to prevent or mitigate misuse. Controversies and allegations were not treated as proof of failure or success, but as additional data points to understand exposure and responsiveness.

Translating findings into investment tools

Rather than treating the results of this analysis as a parallel exercise, the study explored ways to translate qualitative findings into formats compatible with existing investment systems. This led to the development of a structured internal assessment that enabled comparison across companies while retaining the underlying contextual insights.

The purpose of this internal assessment was not to produce a definitive judgement on companies, but to allow human rights risks identified through the study to be reflected more visibly within ESG analysis. Over time, the outputs of the study were integrated into an existing ESG rating framework, allowing company-level human rights considerations, particularly those related to downstream risks, to influence overall ESG assessments.

This integration made it possible to adjust ESG views in a more nuanced manner. Companies with comparable exposure to defence activities could be distinguished based on differences in governance, transparency, risk identification and due diligence practices. In this way, the study informed not only engagement priorities, but also relative risk positioning within portfolios.

Use within investment decision-making

Once integrated, the results of the study became part of the information set used by investment teams. ESG ratings informed by the analysis could be used alongside other criteria to support security selection, weighting decisions or the application of selectivity rules within certain strategies.

Importantly, this approach was not intended to replace engagement, but to reinforce it. By clearly identifying areas of weakness or heightened risk, the study helped articulate engagement expectations and track progress over time. Where risks appeared severe and insufficiently managed, the integration into ESG tools also enabled consideration of stronger investment responses.

Lessons and broader relevance

While this approach was developed in the context of European defence companies, it illustrates how asset managers may seek to **bridge the gap between in-depth human rights due diligence and practical investment decision-making**. The emphasis on context, qualitative judgement and integration into existing systems reflects the view that effective investor due diligence in high-risk sectors requires both depth and operational relevance.

The approach also highlights the importance of flexibility. The elements examined and the way results were integrated evolved over time, reflecting changes in company practices, regulatory expectations and geopolitical contexts. As such, this experience may be useful as an illustration of how asset managers can progressively strengthen their treatment of human rights risks in complex sectors, rather than as a model to be replicated.

Dialogue with public authorities and industry bodies example - France

Within the French context, the Direction Générale de l'armement (DGA) plays a uniquely structuring role. As the authority responsible for procurement, industrial policy, international cooperation and, partly, export licenses, the DGA sits at the intersection of strategic, industrial and regulatory considerations that shape the behaviour of defence companies. Engaging with this institutional environment can therefore contribute to a more nuanced understanding of how ESG expectations, including those related to human rights, can realistically be articulated and integrated across the sector.

Participation in the *Club des investisseurs de la défense*, a working group created by the DGA in 2025, reflects this perspective. This initiative was conceived as a platform to foster dialogue between investors and the French defence ecosystem, with the stated aim of improving mutual understanding between financial actors and defence companies, particularly those within the *Base industrielle et technologique de défense* (BITD). From an investor perspective, such a forum offers an opportunity not only to better understand the specificities of defence business models, funding needs and regulatory constraints, but also to articulate expectations regarding governance, transparency and responsible business conduct in a setting that includes both public authorities and industry stakeholders.

This dialogue is particularly relevant in relation to ESG considerations. The DGA has progressively increased its engagement on issues of transparency, industrial responsibility and sustainability, both through its internal reforms and through its

interactions with industry associations and investors. While ESG considerations are not the primary mandate of the DGA, its central position means that it is often a key interlocutor when discussing how responsible practices can be promoted across the defence value chain, in a manner that remains compatible with strategic and sovereignty objectives.

Industry groupings such as the *Groupeement des Industries Françaises de Défense et de Sécurité Terrestres et Aéroterrestre* (GICAT) also play an important role in this ecosystem. By representing a wide range of defence and security companies, from large primes to SMEs and start-ups, such organisations act as transmission belts between public authorities, industrial actors and, increasingly, external stakeholders concerned with ESG and sustainability. Through thematic working groups, conferences and collective initiatives, these bodies may contribute to the gradual diffusion of best practices on governance, compliance, transparency or risk management, including where these intersect with human rights expectations. Engagement with these platforms can therefore complement company-level due diligence, by offering sector-wide insights and facilitating structured dialogue at scale.

The role of the DGA in the area of arms export transparency is also of particular relevance for investors conducting human rights due diligence. The annual report to Parliament on French arms exports, coordinated under the authority of the Ministry of the Armed Forces, provides a public account of export authorisations, geographic distribution and the policy framework governing these decisions. While such reports do not disclose company- or contract-level risk assessments, they nonetheless offer important context regarding France's stated positions, decision-making criteria and strategic priorities in relation to defence exports. For investors, this information can help frame their own analysis of country and customer risks, as well as their understanding of how state and corporate responsibilities intersect in practice.

In this sense, engagement with the DGA and related institutional actors should not be understood as a substitute for company-level human rights due diligence, nor as an endorsement of specific transactions or policies. Rather, it can be seen as a way to enhance the quality, realism and coherence of investor expectations in a sector where public authorities play a decisive role in shaping market outcomes. By participating in structured dialogue alongside other investors, and by maintaining regular exchanges with both public and industry stakeholders, asset managers may be better positioned to articulate ESG expectations that are informed, credible and grounded in the operational realities of the defence sector.

Additional national level bodies may provide relevant information and support when engaging at the government, policy and system level. For example, the French National Consultative Commission on Human Rights (CNDH) has identified and reported on weaknesses regarding the implementation of the Arms Trade Treaty (ATT)¹⁷. CNDH has put

¹⁷ [A - 2025 - 10 - EN - CNCDH - Opinion Arms Transfers November 2025_0.pdf](#)

forward a series of recommendations addressed to the French Government, Members of Parliament, judges and companies – relating to the ATT and aiming to improve accountability relating to arms transfers. Credible reports such as these from CNDH can help inform priorities and engagement targets for investors.

Note – still to add links and images

Appendix 3: Investors – Understanding Yourself

Prior to considerations of mapping, screening, due diligence or engagement, investors should establish their own context. It is assumed that investors implementing this Guidance have, at a minimum, committed to responsible investment principles.

An internal review may be supported by answering the following questions:

- What is our investment philosophy and how does it relate to defence-related companies?
- What is our current investment strategy as it relates to defence-related companies?
- Where and how are we invested across asset classes?
- Have we fully integrated commitments and processes relating to international standards on business and human rights such as the UNGPs and OECD Guidelines?
- Have we made public commitments on defence or international standards on business and human rights and is our investment strategy consistent with any such statements?
- Does the organisation recognise the financial, reputational, legal and human rights risks associated with defence-related investments?
- Where do we sit in the investment ecosystem?
 - o E.g. asset owner, asset manager, private equity, pre-seed
- Where do we have the most and least leverage and with whom?
 - o E.g. direct holdings, asset managers, indirect holdings
- Are any constraints imposed on us by regulations?
 - o E.g. regulation concerning fund construction and disclosures
 - o E.g. controls, sanctions, extraterritorial legislation etc
- What mandates have we been given from our beneficiaries, clients and owners as they relate to defence investments and responsible investing?
- What is the status of the countries in which we are domiciled or operate (in terms of involvement, or preparedness for, armed conflict)?
- Is there internal or external pressure to change our approach to defence investments?
- Do we have internal expertise on business and human rights, international humanitarian law, international human rights law, international criminal law, conflict, the defence sector, defence technology and dual use products?

By considering these questions, investors will gain an insight into their own context and their strengths and weaknesses when it comes to integrating responsible investment principles for defence-related investments.

Appendix 4: Data providers approaches to controversial weapons

ESG data providers are well placed to support investors by the provision of ‘controversial weapons’ data. These products are generally binary for revenue data (i.e. the company is assessed as making either 0% or >0% revenue from various controversial weapons), although this figure can often be estimated. Companies are regularly divided by data providers into two groups based on whether their products and services are ‘tailor made and essential’ for the lethal use of the weapon or ‘non-tailor made or non-essential’ for lethal use. Exclusions and screening criteria should be clear about the level of involvement that can be accepted, if any.

Example 1 – S&P Global divides its controversial weapons business involvement data into two activities¹⁸:

- *Customized Weapons: This screen covers companies involved in the manufacturing of the components of a weapon. These components are intended solely for use in the production and are essential for the functioning of Anti-personnel Mines, Biological and Chemical Weapons, Blinding Laser Weapons, Cluster Munitions, Depleted Uranium, Incendiary Weapons, and Nuclear Weapons.*
- *Related Products and Services: This screen covers companies that supply products and/or services such as stockpiling and transferring, and sales for Anti-Personnel Mines, Biological and Chemical Weapons, Blinding Laser Weapons, Cluster Munitions, Depleted Uranium and Incendiary Weapons, and Nuclear Weapons.*

Example 2 – FTSE Russell uses Sustainalytics’ Controversial Weapons Radar dataset¹⁹. Their data largely divide into the following, in respect of cluster munitions, anti-personnel landmines, chemical and biological weapons and nuclear weapons:

- *Core Weapons System (directly involved in the core weapon system, or components/services of the core weapon system that are considered tailor-made and essential for the lethal use of these weapons)*
- *Supporting Services (directly involved in providing components/services for a core weapon system, which are either considered not tailor-made or not essential for the lethal use of these weapons)*

The figure below is reproduced from the FTSE Russell website and is included to demonstrate the nuance between data provider definitions:

¹⁸ <https://www.spglobal.com/spdji/en/documents/methodologies/methodology-sp-esg-exclusion-indices.pdf>

¹⁹ <https://research.ftserussell.com/products/index-notices/home/getnotice/?id=2617754>

LONDON CONSULTATION DRAFT GRID – CHAPTER – GUIDANCE – 12 JULY 2026

Weapon Type	FTSE Russell Definition	Sustainalytics Definition
Cluster Munitions (Core Weapons System)	Companies producing cluster munitions and their components, including all precursors, munitions, devices or equipment specifically designed for, and used directly in connection with, these weapons as defined by the 2008 Convention on Cluster Munitions.	Companies directly involved in the core weapon system, or components/services of the core weapon system that are considered tailor-made and essential for the lethal use of these weapons as defined by the 2008 Convention on Cluster Munitions.
Cluster Munitions (Supporting Services)	Secondary products and services specific and critical to cluster munitions as defined by the 2008 Convention on Cluster Munitions	Companies directly involved in providing components/services for a core weapon system, which are either considered not tailor-made or not essential for the lethal use of these weapons as defined by the 2008 Convention on Cluster Munitions
Anti Personnel Landmines (Core Weapons System)	Companies that produce anti-personnel mines as defined by the 1997 Ottawa Anti Personnel Landmine Treaty ¹	Companies directly involved in the core weapon system, or components/services of the core weapon system that are considered tailor-made and essential for the lethal use of these weapons as defined by the 1997 Ottawa Anti Personnel Landmine Treaty. ¹
Anti Personnel Landmines (Supporting Services)	Secondary products and services specific and critical to anti personnel landmines as defined by the 1997 Ottawa Anti Personnel Landmine Treaty ¹ .	Companies directly involved in providing components/services for a core weapon system, which are either considered not tailor-made or not essential for the lethal use of these weapons as defined by the 1997 Ottawa Anti Personnel Landmine Treaty. ¹
Chemical & Biological Weapons (Core Weapons System)	Companies producing chemical or biological weapons and their components, including all precursors, munitions, devices or equipment specifically designed for, and used directly in connection with, these weapons.	Companies directly involved in the core weapon system, or components/services of the core weapon system that are considered tailor-made and essential for the lethal use of these weapons as defined by the 1972 Biological and Toxin Weapons Convention ² and the 1993 Chemical Weapons Convention ³ .
Chemical & Biological Weapons (Supporting Services)	Secondary products and services specific and critical to chemical & biological weapons	Companies directly involved in providing components/services for a core weapon system, which are either considered not tailor-made or not essential for the lethal use of these weapons as defined by the 1972 Biological and Toxin Weapons Convention ² and the 1993 Chemical Weapons Convention ³ .
Nuclear Weapons (Core Weapons System)	Companies that produce nuclear weapons or their components. This includes companies that provide delivery systems (e.g. ballistic missile submarines) or critical services (e.g. maintenance or IT) that are directly related to and specifically designed for nuclear weapons	Companies directly involved in the core weapon system, or components/services of the core weapon system that are considered tailor-made and essential for the lethal use of these weapons as defined by the Treaty of Tlatelolco ⁴ , Nuclear Non-Proliferation Treaty (NPT) ⁵ and the UN Nuclear Ban Treaty ⁶
Nuclear Weapons (Supporting Services)	Secondary products and services specific and critical to nuclear weapons	Companies directly involved in providing components/services for a core weapon system, which are either considered not tailor-made or not essential for the lethal use of these weapons as defined by the Treaty of Tlatelolco ⁴ , Nuclear Non-Proliferation Treaty (NPT) ⁵ and the UN Nuclear Ban Treaty ⁶

Figure 1. Screen shot of FTSE Russell Sustainable Indices - Controversial Weapons exclusions data source change 18 November 2025

Appendix 5: Basis for different elements of controversial weapons definition

Type of controversial weapon	Absolutely Prohibited by Relevant IHL Treaty or Convention? ²⁰	Is treaty signed by investor Country of Domicile?	Is treaty signed by investor client countries of domicile?	Customary IHL (CIHL) mirrors relevant IHL Treaty or Convention?	Revenue data available? Binary or %?	Considerations for companies involved in tailor made or essential parts or services for core weapon system	Considerations for companies involved in non-tailor made or non-essential parts of services for core weapon system	Conclusion
Biological Weapons	Absolutely Prohibited ²¹ Geneva Protocols, Biological Weapons Convention			Yes Rule 73				
Chemical Weapons	Absolutely Prohibited Geneva Protocols, Chemical Weapons Convention			Yes Rule 74				
Cluster Munitions	Absolutely Prohibited Convention on Cluster Munitions			No - Insufficient consensus as to whether weapon is inherently prohibited by CIHL (Rule 71). CIHL (Rule 81) notes particular care must be taken to minimise indiscriminate effects.				
Anti-personnel landmines	Absolutely Prohibited Anti-Personnel Mine Ban Convention			No – Multiple States use landmines. CIHL (Rule 81) notes particular care must be taken to minimise indiscriminate effects.				
Nuclear Weapons	Absolutely Prohibited by Treaty on the Prohibition of Nuclear Weapons			No – multiple States have nuclear weapons. Insufficient consensus				

²⁰ This is a complex area and this column is a highly simplified list, with a focus on bans relating to development, production, stockpiling and acquisition of weapons, as opposed to covering prohibitions on weapon use.

²¹ Meaning State parties have agreed to not develop, produce, acquire, stockpile, retain, transfer or use the weapon

LONDON CONSULTATION DRAFT GRID – CHAPTER – GUIDANCE – 12 JULY 2026

Type of controversial weapon	Absolutely Prohibited by Relevant IHL Treaty or Convention? ²⁰	Is treaty signed by investor Country of Domicile?	Is treaty signed by investor client countries of domicile?	Customary IHL (CIHL) mirrors relevant IHL Treaty or Convention?	Revenue data available? Binary or %?	Considerations for companies involved in tailor made or essential parts or services for core weapon system	Considerations for companies involved in non-tailor made or non-essential parts of services for core weapon system	Conclusion
	(Note Limited prohibition in Non-Proliferation Treaty)			as to whether weapon is inherently prohibited by CIHL (Rule 71).				
Incendiary Weapons	Not Absolutely Prohibited – Use regulated by Convention on Certain Conventional Weapons (CCW) Protocol III			Yes - Prohibitions on certain uses. Rule 85				
Non-Detectable Fragment Weapons	Not Absolutely Prohibited – Use prohibited by CCW Protocol I			Yes – Prohibitions on use. Rule 79				
Expanding bullets	Not Absolutely Prohibited - Use prohibited Hague Declaration (IV,3) 1899			Yes - Use of expanding bullets is prohibited Rule 77				
Exploding bullets	Not Absolutely Prohibited – Use prohibited St Petersburg Declaration 1868			Yes – Use of exploding bullets is prohibited Rule 78				
Blinding Laser Weapons	Partial – CCW Protocol IV prohibits use and transfer, not development.			Partial - Use prohibited Rule 86				
Autonomous Weapons ²²	No specific treaty or convention yet. Still covered by CCW.	NA		NA – But use must be used in accordance with C-IHL Rules				

²² Autonomous weapons are included as they have been raised as the ‘next frontier’ of controversial weapons and they are part of discussions about the regulation of autonomous and AI enabled weapons. See [ICRC position on autonomous weapon systems | ICRC](#)

Appendix 6: Setting business thresholds in exclusions

When setting their approach to exclusions, investors will need to choose which categories and groupings of business activities, services, products or business models are relevant for their exclusions. For managers with concentrated portfolios, these internal definitions may be directly translated into exclusions. However, for many investors the day-to-day implementation of exclusions may depend on the categories used by their managers or data providers.

Example A - Investor has a 5% revenue threshold for companies with ‘any military contracting revenue’.

Practical questions for investor to ask themselves:

- What kinds of military contracting are in scope of restrictions e.g. providing weapons, weapon platforms, engineering support, civilian IT equipment, catering services, construction services, training or educational support?
- Have we justified why weapons companies are treated in the same way as catering service companies by this approach?
- Does this only cover companies with direct contracts with the *military/government*, or with the wider defence ecosystem?

Example B - Investor has a 10% revenue threshold for companies involved in conventional weapons and 0% for controversial weapons.

Practical questions for investor to ask themselves:

- Do the definitions of “conventional weapons”, “controversial weapons” and “weapons” in general used by both the manager and the data provider they rely on align with our own?
- Do we consider that ‘conventional weapons’ restrictions extend to non-essential and non-tailor-made products and services for controversial weapons - or are these permissible investments?

While some companies are set up to be ‘defence-first’, other companies will explore defence revenue as they grow and evolve. Private market investors, in particular, are encouraged to explore and set red lines, both from an organisational perspective and within specific funds. In the earliest stages of investment, revenue thresholds will probably not be an appropriate approach. However, it is particularly important to understand how both the company and the asset manager, if relevant, categorises defence-related companies and activities.

Revenue threshold screens

Where investors wish to avoid allocating capital to defence-related companies, this is often delivered by excluding companies based on the revenue they derive from defence-related activities. This table explores the pros and cons of different thresholds:

THRESHOLD	PROS	CONS	COMMENT
0%	Clear logic. Easy to explain. Removes any involvement and connection to potential serious harms or violations.	Restricts an ever increasing % of investible universe including companies with marginal defence revenue.	Total % of restricted universe will need to be considered. Potentially more appropriate for companies involved in weapons that don't align with IHL.
Minimal (e.g. 1-2%) revenues	Strong signal that it is not a desired investment. Avoids excluding companies which make a minimal proportion of revenue from defence.	Small revenue levels do not preclude involvement in products or services with significant risks and impacts. Accuracy of defence revenue data is questionable.	Increases the size of the public investible universe compared with 0% level. Maybe more appropriate for investors who wish to limit exposure as much as possible but guard against inadvertent breach of a 0% threshold.
'Material' 5-10%	Explainable approach without capturing too many companies for whom defence is arguably not material or a main part of their business.	Significantly increase exposure to companies with defence revenue, requiring a step change in due diligence to identify and act on risks.	Pragmatic approach for investors wishing to avoid exposure to defence focused companies without overly limiting the investible universe.
25%	Increased flexibility, maintaining access to companies who make substantial revenues from defence.	As above, plus it becomes harder for the investor to say it doesn't invest in defence.	May be suitable for investors wishing to avoid companies whose 'main business' is defence related.
50%	Limited impact on investible universe. Provides narrative that the investor 'excludes companies who make the majority of their money from defence' but retains the flexibility to invest in companies with wider roles in society.	As above.	Still excludes all the 'pure play' defence companies so may be useful for mandates where they want to avoid 'defence first' exposure.

Appendix 7: Due diligence tools

A. Company defence-related revenue

This information assists in determining the scale of the company's exposure to the defence sector. It may also be required to ensure adherence to investor exclusions/restrictions based on revenue.

Topic	Due Diligence Questions										Consideration									
Revenue	What proportion of the company's revenues derive from defence related products and services?										While small proportions of revenues do not preclude defence-related risks, they may change investor views on what to expect from companies.									
	Is it growing or shrinking?										Increasing reliance on defence revenue increases the investment risks relating to a compliance failure, loss of export licence, sudden contractual changes etc.									
%	0	1	2	3	4	5	10	15	20	25	30	40	50	60	70	80	90	100		
Trend																				
Size of holding and importance to portfolio/company	How large is the holding? Is the company material to the investor fund, portfolio or index? Is the holding size material to the company?										Increased holding sizes increase both the expectations of and potential for leverage with the company. Investments which are individually material to the fund may be hard to exit. Concentrated positions can magnify the impact of legal, financial, reputational and human rights incidents.									
Importance to investor ²³	Very Low			Low			Medium				High			Very High						
Importance of defence revenue to company ²⁴	Very Low			Low			Medium				High			Very High						

²³ i.e. how important is the company to the investor overall, or e.g. within a specific fund. While a single company may not be important to a passive index fund, a large-tech company may be material even in a diversified public equity portfolio. A small private markets fund may consider each company strategically important to the success of the fund.

²⁴ This goes beyond just the financial materiality of the revenue. A company making a material % of revenue from defence would consider it important to business success, but a company may also be a strategic or key provider to national security and while the revenue may be de-minimis, the impact of withdrawing from defence may be significant. This category aims to quantify the importance of defence revenue to the company.

B. Defence-related products and services

This section addresses a key aspect of risk, namely the types of defence-related products or services that the company is involved with and its position in the value chain. For some investors, this will be the most important factor and a threshold question for whether the company is within its investible universe.

Topic	Due Diligence Questions	Consideration
Position in ecosystem	Where does the company sit on the GRID mapping? See image in the Introduction section.	The company's relationship with governments and militaries, as well as its role in the export chain, will inform the leverage and limitations it operates under.
Nature of activities, products and technologies	What are the company's defence related products and services? E.g. ▪ Platforms (e.g. aircraft, naval vessels, armoured vehicles) ▪ Weapons systems and subsystems ▪ Parts for platforms, weapons systems. ▪ Services (maintenance, training, logistics, intelligence support). ▪ Enabling or dual-use technologies (e.g. surveillance, cybersecurity, artificial intelligence, decision support services).	Platform, weapon systems and C2 integrators, plus sub-prime contractors providing support services, are likely the most proximate to potential IHL violations and adverse impacts and investors may wish to prioritise them in terms of highest inherent risk.
	Are the products 'conventional arms' ²⁵ or the parts or components required to manufacture them?	Conventional arms fall under the scope of the Arms Trade Treaty . Investors may wish to highlight products which are fall under the scope of the ATT.
	Can the products be used to directly kill or injure people e.g. missiles?	Investors may wish to prioritise companies whose products are most visibly involved in kinetic military action / combat in terms of inherent risk.
	Does the company have involvement in weapons prohibited by customary IHL or relevant IHL Treaties?	Involvement in these products should raise immediate caution flags for investors.
	Does the company have involvement in other controversial weapons?	

²⁵ Conventional arms include tanks, armoured combat vehicles, large calibre artillery systems, combat aircraft and unmanned combat aerial vehicles, attack helicopters and unmanned rotary wing combat vehicles, warships, missiles and missile launchers, small arms and light weapons.

Topic	Due Diligence Questions			Consideration	
	Does the company provide contractual services to the military which directly or indirectly support combat operations?			The level and type of involvement is important as it will dictate how involved companies and their staff may be to IHL breaches and also determines whether the company and its staff may be classed as legitimate military targets.	
	Do the products or services have inherently high human rights risks e.g. surveillance technology?			Certain products and services can support repression, oppression and the restriction of fundamental rights, which elevates the inherent risks.	
Inherent risk	Very Low	Low	Medium	High	Very High

C. Geographic footprint and CAHRA exposure

The potential investee company's geographic footprint will determine the legal controls that it is already subject to, including export licensing, and the enforcement of those controls (note separate consideration of regulatory factors below). The company's footprint will also be relevant to risks associated with its counterparties, including governments.

Topic	Due Diligence Questions			Consideration	
Geographic footprint & operating context	Where does the company operate in terms of the manufacturing and sale of products and the provision of services?			Some operating contexts may be inherently high risk in terms of government / user conduct.	
	What is the exposure to conflict-affected or high-risk areas, including through operations, exports, maintenance contracts, joint programmes or other support?			Significant exposure to high-risk areas increases the likelihood of legal, financial, reputational and human rights risks.	
	What is the duration and nature of the exposure to conflict-affected and high-risk areas?			One-off contracts reduce the likelihood of ongoing involvement in problematic activities.	
	Do any of the operating countries or contexts raise significant concerns relating to human rights violations and IHL breaches?			Alleged or confirmed recent and current human rights violations and IHL breaches will elevate the context risk significantly.	
	Are the countries where products are being exported to resilient in terms of bribery and corruption risks?			Countries with higher levels of corruption may increase the risk of end-use diversion.	
Geography / context risk	Very Low	Low	Medium	High	Very High

D. Applicable regulatory and legal frameworks

Export licensing regimes may incorporate human rights elements into the criteria for licence applications. Consideration of the licence application will therefore include a degree of due diligence. While unlikely to be sufficient to meet responsible investment mandates, such regimes provide a starting point for further diligence.

Topic	Due Diligence Questions	Consideration
Export control context	Which geographic areas are subject to export controls e.g. USA, EU, Japan, UK?	The regulatory context can be significantly different across operations, with implications for the quality of government controls and oversight.
	Have those countries ratified the Arms Trade Treaty (ATT ²⁶)?	Ratification of the ATT may be used by investors as a useful proxy for understanding the presence of robust export controls (or at least the commitment to implement them) ²⁷ . Investors may wish to use non-ratification as a flag for increased due diligence.
	Do the company's products fall under the scope of the ATT?	
	Does the company fall under 'dual-use' or 'strategic export controls'?	
	Does the company fall under 'military / defence export licensing' rules?	
	Do the export licensing criteria include human rights considerations?	A group of countries including several European countries, Australia, Canada, Japan, New Zealand, Republic of Korea, the UK and the US are

²⁶ The [Arms Trade Treaty](#) 2013 regulates the international transfer of conventional arms (from tanks and aircraft to small arms, ammunition and the parts/components to manufacture them). It establishes common standards for export authorisation and prohibits arms transfer authorisation to states if the transfer would, inter alia, violate UN Security Council arms embargoes or if the state has knowledge at the time of authorisation that the exports would be used in the commission of genocide, crimes against humanity, or war crimes and attacks on civilian objects and protected civilians. Signatories and ratification states can be found here [treaty-status | The Arms Trade Treaty](#).

²⁷ Several important countries for arms exports are signatories to the ATT, but have not ratified it, meaning they are not legally bound in the same way as states who have ratified it. These include Israel, Turkey, Ukraine, the United Arab Emirates and the United States of America. Significant non-signatories include India and the Russian Federation.

Topic	Due Diligence Questions			Consideration	
				party to the Export Controls and Human Rights Initiative Code of Conduct which requires them to take human rights into account in reviewing licensing applications. It may not be possible to access criteria in all countries.	
	Does the company fall under anti-boycott legislation?			Some companies may be legally prevented from participating in unauthorised foreign boycotts e.g. of non-military products or services.	
Government role in sales	Is the government the seller of record? Does the government engage in government-to-government sales, support negotiations, provide guarantees or take ownership of export risk?			Foreign military sales / G-to-G programmes may add a layer of complexity and reduce direct contractual exposure for companies to downstream harms. Companies may also believe that these processes provide safe-harbour from litigation or responsibility. Government involvement provides important context for investors.	
Export control risks	Are there concerns about the quality of the export controls in relevant operational countries?			Based on the context, investors may wish to assign a risk categorisation for the company export context.	
Export control risk	Very Low	Low	Medium	High	Very High

E. Customers, end-users and business relationships

Customer risks are highest where there is inadequate transparency over the identity of the customer or end-user. While the risk of product diversion to unknown end-users cannot be wholly eliminated, it is heightened when geographic factors are also a risk. (See also section above for considerations regarding government-to-government supplies.)

Topic	Due Diligence Questions	Consideration		
Customers and business relationships	Who are company's customers across the following categories: - Government Ministry - State owned entity - Armed services / defence force - Other defence-related companies - Intermediaries / resellers - Private security company (PSC) - Other - Unknown	Contractual counterparties have implications for leverage and control. While specifics may not be available, knowing if they only sell business-to-business helps set the context. Lack of visibility is likely to prompt further questions.		
	Gov't	SOE	Armed Forces	B2B
	Intermed/Reseller	PSC	Other	Unknown
	Is the company involved in major national or international defence programmes or initiatives?	Involvement in these programmes may impact company ability to build and use leverage where there are human rights concerns.		
End users	Who are the end-users of the products or services: - Government Ministry - State owned entity - Armed services / defence force - Other defence-related companies - Private security company - Other	End user risk is a key issue for defence due diligence. Note – for equipment used to manufacture goods, the end-user is the manufacturer. Lack of visibility is likely to prompt further questions.		
	Gov't	SOE	Armed Forces	B2B
	Intermed/Reseller	PSC	Other	Unknown
Customer, Business Relationship and End User Risks	What exposure does the company have to customers or end users with weak human rights and bribery/corruption records, histories of misuse or diversion? What exposure does the company have to customers or end users who are involved in conflicts?		Having established the customers, business relationships and end-users, these can be matched to concerns about conduct to give a view of customer, business relationship and end user risks.	
	Risk Area		Level of Concern	
	Human rights record		Low	Medium
	Bribery & corruption record		Low	Medium
	Product misuse record		Low	Medium
	Product diversion record		Low	Medium
	Current conflict involvement		Low	Medium

F. Controversies

Controversies are where the legal, financial and human rights risks outlined above crystallise. It may not be the case that a single controversy indicates that a company is uninvestible; due diligence should look to establish whether a controversy indicates a systemic issue around risk management and mitigation or a one-off event. Even when they do not translate into significant media stories or reputational risks for the investor, controversies should be given significant weight in understanding the company context.

Topic	Due Diligence Questions			Consideration	
Controversies	Are there current or recent controversies connected with: - Bribery and corruption - Export licensing compliance, sanctions, intermediaries - Product use and misuse including connections to alleged breaches of IHL, or International Crimes - Product diversion - Criminal or civil cases against the company relating to the above - OECD National Contact Point complaints or cases			Is the same weight given to an allegation as an incident or event that has been the subject of a legal decision? Both carry reputational risks. Consider nature of the controversy and severity of alleged harm.	
	Are the products or services being used by a government or country who has an <i>alleged</i> track record of: - Invading other states or attacking other states in violation of the UN Charter - Engaged in illegal occupation or annexation of another State or its territories - Perpetrating crimes against humanity, war crimes or genocide				
	Has the company been caught up in reputational scandals or controversies due to its products, services, subsidiaries, partners or affiliates?			Significant media stories and reputational risks are not necessarily proportionate to the company’s involvement or connection with downstream incidents, but they can translate into significant reputational concerns for the investor.	
Controversy severity	Very Low	Low	Medium	High	Very High

Risk management and mitigation

Policies and procedures to manage risk should be assessed together, as two critical elements of risk management and mitigation. A policy without a supporting process is highly unlikely to be effective in managing risk, whereas a process without a policy may be somewhat effective while lacking full transparency and potentially consistency.

It should be recognised that data may be more readily available for listed companies, and early-stage companies are less likely to have comprehensive policy suites. Investors will need to tailor their due diligence to the maturity of the company (i.e. from pre-seed investment to publicly listed companies).

Continues on next page

G. Assessing company policies

Topic	Due Diligence Questions			Consideration	
Avoiding legal complicity	Has the company expressed a clear policy-level commitment to supporting the principles of IHL?			The extent to which companies can be expected to manage complicity risks will depend on their position in the value chain. Companies which are involved with products which can directly kill or injure people should be expected to be aware of complicity risks, even where they are at an early stage, or where this is not their core business.	
	Is the policy commitment public?				
	Is the policy overseen at the most senior level of the company?				
Respect for human rights	Has the company expressed a clear policy-level commitment to respect all internationally recognised human rights?			Policies should be interrogated where available to determine whether they address only human rights in the company’s operations and supply chain or also consider the wider value chain including end use. Human rights elements may also be present in responsible business policies or similar.	
	Does the commitment apply to the whole value chain, or explicitly cover downstream activities, customers and users/use, and conflict-affected contexts?				
	Is the policy commitment public?				
	Is the policy overseen at the most senior level of the company?				
Anti-bribery and corruption	Has the company made a policy-level commitment to the prohibition and elimination of all forms of bribery and corruption in their business operations and business relationships, applying to all business partners and across all jurisdictions?			ABC policies are commonplace in many jurisdictions and would be expected for most companies (potentially even earlier stage).	
	Is the policy commitment public?				
	Is the policy overseen at the most senior level of the company?				
Political advocacy and lobbying	Does the company have a transparent approach to lobbying, political advocacy or political donations?			Not all companies engage in lobbying and this should not necessarily be a negative indicator.	
Alignment with policy expectations	Full	Useful	Some gaps	Poor	Absent

H. Assessing company processes

The company should support its policies with robust and well implemented processes. Much of this information will not be public and accessing it for public markets and certain private markets strategies may be challenging. Aspects may need to be addressed as part of an engagement strategy, where possible, if sufficient comfort can be obtained through other due diligence aspects to inform a positive investment decision. The earlier stage the company, the less likely they are to have these robustly documented processes, so the investor will need to tailor the due diligence questions and expectations for the type of company being reviewed.

Topic	Due Diligence Questions
Legal complicity risk management	Does the company recognise legal complicity risks relating to their own business operations and the wider context of use and misuse of their products and services?
	Is there a formal system identify and manage legal complicity risks and who within the organisation is responsible for the system(s)?
	How are IHL risks integrated into the design, development and production of products and services?
	How are IHL risk considerations integrated into sales contracts, customer due diligence and service contracts?
	How are IHL risks monitored, escalated and acted on once products have been sold or once services are underway?
	What does the company understand are its key legal complicity/IHL risks? Does the company demonstrate it has sufficiently mitigated these risks?
	Is it clear how the complicity risk management interacts with human rights due diligence processes?
Human rights due diligence	Does the company explain its processes for identifying, analysing, avoiding, mitigating and remediating adverse human rights impacts, plus tracking and measuring performance and communicating progress?
	Is it clear how their HRDD process applies to their defence-related products and services, specifically for product design, export/sale and downstream use and misuse?
	Does the company recognise product use/misuse as a salient human rights risk?
	And what are the specific risks the company believes it is exposed to?
	How does the company engage with stakeholders as part of its approach to respecting human rights?
	Does the company have a process to identify and engage with potentially impacted stakeholder on the ground?
	Does the company explain its approach to providing or enabling access to remedy where it has caused or contributed to a negative impact?
	How does the company modify its approach to deal with conflict affected and high-risk areas if relevant to their context (e.g. Heightened Human Rights Due Diligence)?

Topic	Due Diligence Questions
Anti-bribery and corruption management systems	Does the company demonstrate a robust, risk based anti-bribery and corruption management system? Are whistleblowers formally protected from retaliation?
Contractual Controls	How does the company conduct due diligence on the sale or purchase of products and/or services to/from third parties to avoid or mitigate human rights, legal, reputational and financial risks and impacts covering: - The extent of any legal licensing requirements [and sanctions] - The risk profile of the direct customer / client including historical transactions, length of relationship and previous controversies involving the counterparty - The risk profile of the country of destination, including its involvement in armed conflict or military occupation, levels of authoritarianism, and levels of public sector corruption - Likely end use of the specific products or services - Likely end user of the specific products or services - Diversion risks for products or services - Any ongoing support or maintenance relationships - The current and potential leverage of the company with its clients, customers or end users - Intended or foreseeable disposal or decommissioning of products or service Does the company incorporate contractual clauses about appropriate use of weapons? Does the company set standards for terminating contracts based on e.g. IHL breaches, transfer or diversion? Does the company incorporate considerations for remedy in contracts?
Mitigating processes	Does the company implement any of the following actions: • Training internal staff, executives and board members on relevant risks and company systems. • Obtaining and maintaining relevant security clearances for staff. • The inclusion of strict end-use, resale, transparency and auditing clauses, as well as the right to suspend or terminate contracts or services if evidence emerges of misuse or diversion, in contracts. • Integrating risk aggregators, human rights red flags, and other types of open-source intelligence into KYC due diligence, moving beyond a “compliance only” framework. Integrating a “lawful-by-design” approach at each stage of the product life cycle, from R&D to end use. • Through life monitoring and investigation of potential misuse and contractual breaches and ensuring information feeds back into decision making such as contract renewal, provision of spare parts or ongoing maintenance and support services*. • Training staff in the lawful use of equipment or services.
Political advocacy and lobbying controls	Does the company demonstrate a system to manage improper advantage risks, including tracking and monitoring payments, gifts, hospitality, political or charitable donations, and engagements with political actors, partners, advisors, and intermediaries?

Topic	Due Diligence Questions				
Expertise	Does the company demonstrate sufficient knowledge and expertise on key issues such as IHL, complicity risks, export regimes and human rights due diligence? How is relevant expertise obtained (e.g. from outside the company)?				
Broader governance	Does the company's broader approach indicate that it manages governance effectively?				
Alignment with process expectations	Full	Useful	Some gaps	Poor	Absent

Next steps

Based on the outputs of the due diligence tools, investors can develop a qualitative view of the company to inform decisions on whether to invest, avoid investment, conduct further due diligence, engage, divest or monitor the company.

Additional due diligence, potentially via company engagement, may need to be carried out based on the specific risk context. It may be that companies fail to supply sufficient information for a proper assessment of the risks and mitigations in place at the pre-investment stage; the following section on engagement during the holding period addresses a post-investment strategy to engage with the company to ensure that risks are minimised during the holding period.

Appendix 8: Engagement questions for companies

Due Diligence Theme	Engagement Questions
Defence-related products & services	• How are human rights and IHL considerations integrated into product design and development? • For high-risk categories (surveillance, ISR, command-and-control, cyber, AI-enabled systems), what safeguards are built into design, deployment, training and servicing to reduce foreseeable misuse? • Are there technical constraints, logging/auditability features, geofencing, access controls, or disablement mechanisms and what governance controls their use? • How are foreseeable misuse risks assessed for defence and dual-use products and services, and what safeguards are built into design, deployment, training and servicing, particularly where products/services relate to high-risk categories such as surveillance, ISR, command-and-control, cyber or AI-enabled systems? • How does the company assess dual-use drift (capabilities used in ways not intended at sale)?
Geographic footprint and conflict exposure	• What framework does the company use to determine its tolerance for operating in or selling products to be used in conflict-affected or high-risk settings, including situations of military occupation? • How are contextual risk assessments updated as conflict dynamics shift?
Applicable regulatory and legal frameworks	• How does the company's hHRDD go beyond export licence compliance, and can it evidence transactions it has declined, restricted, or applied stricter conditions to than the licensing authority required? • How does the company ensure compliance processes remain effective across jurisdictions where domestic law may differ or enforcement may be weak? • How does the company manage risks of circumvention of export controls or sanctions through third parties, intermediaries, offshore structures, or onward transfers? • How does the company navigate cases where it has less visibility (e.g. government-to-government sales)?
Customers, end-users and business relationships	• How are customer risk profiles (including human rights and IHL considerations) incorporated into decisions to bid, contract, deliver, maintain, upgrade, provide spares, or renew support services? • How does the company assess the human rights track record of government/security customers, including where there are credible allegations of serious harm? • How does the company assess and document end-use, end-user and diversion risks for specific products and services, including where there are multiple transfer layers (e.g. integrators, resellers, government-to-government arrangements)?

Due Diligence Theme	Engagement Questions
	• <i>Ask for examples:</i> a case where the company declined, paused, restricted, or exited a customer relationship due to end-use or conduct concerns.
Controversies	• What processes exist to identify, assess and respond to credible allegations that products, services or business relationships have been linked to serious harm, and how do outcomes inform future decisions, remediation and disclosure? • If credible allegations arise after delivery, what is the internal process to assess them, determine whether they relate to the company's products/services, and decide response options? • What information can the company disclose publicly, and what can be shared confidentially with investors, to demonstrate that risk controls are robust while recognising legitimate security and contractual constraints? • <i>Ask for examples:</i> To support a meaningful discussion of how these processes operate in practice, request examples that demonstrate (i) what happened, (ii) what the company did, (iii) what changed as a result, and (iv) what can be evidenced.
Assessing company policies	• How is oversight of human rights, IHL and legal complicity risks structured (including board accountability, senior executive responsibilities and escalation pathways for high-risk sales and ongoing support decisions)? • What training is provided across functions on conflict and legal (IHL/IHRL) expectations relevant to the company's products and services?
Legal complicity risk management	• Where do sanctions/export-control compliance and human rights / IHL / IHRL / ICL risk governance intersect in decision-making (e.g. who resolves conflicts between "legal to sell" and "high risk to people")?
Human Rights Due Diligence	• What is the company's human rights due diligence (HRDD) approach for downstream product use/misuse risks? • When does the company apply heightened (h)HRDD for CAHRA-linked contexts, and how is that threshold defined operationally? • How does the company engage stakeholders (including civil society) to understand contextual risk and impacts linked to product use/misuse, especially in high-risk contexts? • How does the company enable grievance mechanisms and access to remedy for affected stakeholders, including in higher-risk contexts where accessibility, security and retaliation risks may be elevated?
Contractual Controls	• What contractual controls and leverage are used to prevent or mitigate adverse impacts (e.g. end-use restrictions, audit and reporting rights, suspension/termination triggers), and what criteria determine when the company will restrict support, suspend delivery, or disengage? • What leverage exists after delivery (spares, maintenance, upgrades, software updates, training, warranties), and how is it governed?

Appendix 9: Factors to bear in mind in assessing arms export regimes

Key assessment areas for investors	
Questions to ask	Potential indicators
Export control framework - Is the exporting State a party of the Arms Trade Treaty (ATT)? - How have ATT obligations been transposed into domestic law? - Are human rights and IHL explicitly included among export licensing criteria? - Is there a formal risk assessment process? - Are there mechanisms for licence suspension and review when circumstances change? - Are denial decisions shared or coordinated with other countries (e.g. within the EU)?	- Existence of legally binding human rights/IHL criteria - Transparency of decision-making - Publication of annual arms export reports - Parliamentary oversight mechanisms - Judicial review possibilities
Human rights and IHL integration - Which government departments participate in licensing decisions? - Is legal expertise on IHL formally integrated into the process? - Does the assessment rely on information from diplomatic missions, intelligence services, international organisations or NGOs? - Are civilian harm, diversion risks and patterns of past misuse considered? - Is there evidence that licences have been denied, suspended or revoked on human rights or IHL grounds?	- Reference to IHL and human rights in official guidance. - Public licence denials. - Independent court decisions challenging licensing practices. - Government reviews following conflict-related controversies.
Strategic and geopolitical context - Is the State pursuing an explicit defence export promotion strategy? - How important are arms exports to its industrial base and strategic autonomy? - Does the country maintain particularly close security relationships with certain regions or recipient States? - Are exports used as instruments of foreign policy or defence cooperation? - Are there direct government-to-government sales mechanisms?	- National defence industrial strategy documents - Major bilateral defence agreements - Government statements regarding key export markets - Export concentration by destination
Indicators investors may wish to examine - Heavy reliance on exports to conflict-affected countries. - Significant exposure to jurisdictions repeatedly criticised by UN bodies or NGOs. - Recurring controversies despite formally authorised exports. - Large dependence on a single government customer or region. - Weak transparency around export destinations. - Repeated allegations of misuse of supplied equipment. - Evidence that the company's commercial strategy depends on markets facing heightened human rights or IHL concerns.	

Useful sources and databases

- [Arms Trade Treaty](#): Treaty text, State Parties, National implementation reports, Conference of States Parties documentation.
- National or regional frameworks:
 - o E.g.: EU Common Position on Arms Export
- [SIPRI Arms Transfers Database](#): Tracking major weapons transfers, identifying key suppliers and recipients, mapping customer exposure, understanding historical export patterns.
- [SIPRI Yearbook](#): Conflict analysis, military expenditure, arms trade trends, regional security dynamics.
- [International Committee of the Red Cross](#): IHL interpretation, conflict classification, humanitarian concerns linked to weapons use.
- [Conflict Armament Research](#): Diversion investigations, weapon tracing, unauthorised end-use findings.
- NGOs such as Amnesty International, Human Rights Watch, PAX, Saferworld, International Peace Information Service (IPIS): Recipient-country risk assessment, documentation of alleged misuse, analysis of arms transfer controversies.