SEPTEMBER 2026

DefenceTech Materiality Napkin

REFRAME VENTURE

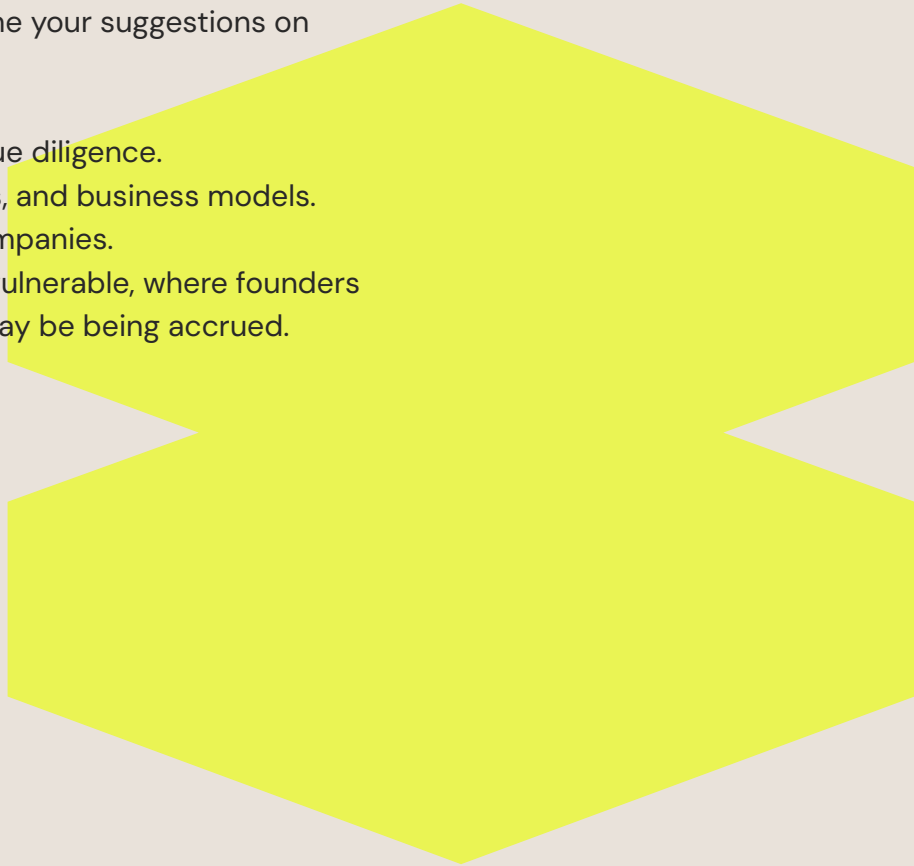
Contents

How to use this guide	03
Theme 1: Product & Supply Chain	04
Theme 2: Customers	05
Theme 3: Security	06
Theme 4: Governance & Compliance	07
Theme 5: Operations & Environment	08
Theme 6: AI & Autonomy	09

How to use this guide

This framework is a v1 due-diligence tool developed with international input from GPs, LPs, operators, and domain experts. This is an evolving project and will continue to incorporate other sectors of the defence industry including space, quantum and biotechnology. We welcome your suggestions on both content and format.

- Use the tool to identify material factors for prospective companies in due diligence.
- What is material will depend on sector sensitivities, stage and resources, and business models.
- The questions are not pass/fail, and this is not a checklist to send to companies.
- The questions are designed to identify where companies are strong or vulnerable, where founders are thoughtfully engaged or have blind spots, and where unseen debt may be being accrued.



Theme 1: Product & Supply Chain

Defence technologies face unique product design, testing, verification, validation and assurance requirements. A missing assurance standard or product certification can make a company ineligible to bid a contract. Shifting geopolitical alliances can also affect supply chains from critical minerals through to parts for manufacturing for critical components. Technologies with defence applications also face unique IP risks, including a secrecy order that can limit the commercial pathway for a promising dual-use technology

CATEGORY	WHY IT MATTERS & ASSOCIATED RISKS	CONTEXT & BUSINESS CASE	FUNDING STAGE	DUE DILIGENCE QUESTIONS
1.1 INTELLECTUAL PROPERTY & SECRECY ORDERS	• Patents on dual-use / frontier tech are reviewed for national-security implications and may receive a Secrecy Order that restricts disclosure, sale or export. • A Secrecy Order can foreclose commercial / dual-use markets and delay or block fundraising and partnerships.	IP position is core to defensibility and valuation.	Very early, Early	• How central is patent / IP protection to your moat and business model, and what is the current filing status? • Which of your filings touch technologies plausibly subject to a Secrecy Order, and what is your read on that risk? • If a Secrecy Order were imposed, how would it change your addressable market and exit options? • How are you protecting trade secrets and know-how where patenting would force disclosure?
1.2 PRODUCT QUALITY & STANDARDS	• Failure to meet required industry / customer standards can make a company ineligible to bid, trigger contract non-renewal, or create product-liability exposure and fines. • Weak quality systems undermine customer trust and slow adoption.	Certifications and standards compliance are often gating criteria for contracts	Early, Growth	• What distinguishes your product technically, and which quality standards (ISO, NIST, sector-specific) are you certifying to and by when? • Which standards are contractually required by your target customers vs. voluntary, and where are the gaps today? • What safeguarding features protect operators and end-users, and how are they validated? • Who owns quality compliance internally and how is it resourced?
1.3 SUPPLY CHAINS	• Reliance on concentrated or single-source suppliers creates single points of failure. • Exposure to geopolitical shocks: tariffs, export bans, critical-mineral shortages. • Human-rights abuses, forced labour, pollution or bribery in the chain create compliance breaches, reputational damage and operational slow-downs.	Supply-chain mapping gives transparency over where components are sourced. Procurements favour or require NATO-ally sourcing to be eligible to bid .	Early, Growth	• What are the key components in your supply chain (Tiers 1–4) and where each is sourced vs. where it could be sourced. • Which components are single-sourced or concentrated in one geography, and what is your alternative-sourcing plan? • How do your target customers' sovereignty requirements shape your sourcing, and what does that cost you commercially? • How do you screen and monitor suppliers for environmental and social risk (modern slavery, wage theft, pollution, bribery)? • Which bottlenecks or regulatory changes could disrupt procurement, and how are you mitigating them?

Theme 2: Customers

Defence and dual-use companies need to be able to say not only who they sell to, but who they will not sell to—and how those boundaries will be explicitly enforced when revenue is on the line. Certain countries have compliance-based processes that must be followed for Export Controls and End-use Monitoring (EUMs). Other processes including Know Your Customer Due Diligence (KYC) and Human Rights Due Diligence (HRDD) can provide an extra level of security. These all address the same underlying issue: whether the company has a credible system for preventing diversion, misuse or sales into contexts where the technology could enable serious harm.

CATEGORY	WHY IT MATTERS & ASSOCIATED RISKS	CONTEXT & BUSINESS CASE	FUNDING STAGE	DUE DILIGENCE QUESTIONS
2.1 CUSTOMER TYPES (SEGMENT SCREENING)	• Selling into the wrong segments or geographies risks products reaching terrorists, criminals, non-state actors or entities likely to violate international law / human-rights norms. • Weak segment policy creates diversion, reputational and legal exposure.	Clear, enforced segment policies make the company investable and lower diligence cost for acquirers and co-investors.	All	• SCREENING: Which segments do you serve or plan to – military, intelligence, law enforcement, private security, wholesale/secondary markets, direct-to-consumer? In which geographies for each? • Where do you draw red lines on segments or geographies, and how do you enforce them in practice? • How do you handle secondary-market / distributor sales where end-users are harder to see?
2.2 KNOW YOUR CUSTOMER (KYC) DUE DILIGENCE	• Without KYC, military / dual-use products can be diverted to adversaries, terrorists or sanctioned entities. • Failure exposes the company to sanctions breaches, criminal liability and reputational collapse.	Robust KYC is a license-to-operate for defence sales and a prerequisite for scaling into new customers/ geographies. Its absence is a red flag that can kill deals in diligence.	Growth	• What is your KYC process for non-state customers – what identity and beneficial-ownership checks do you run, and using which sources? • What red flags trigger enhanced review or a no-sale decision, and who signs off? • How do you screen against sanctions and watchlists, and how often is it refreshed? • Who owns KYC internally and how is it resourced as you scale?
2.3 EXPORT CONTROLS	• Export licenses are required to sell military and most dual-use across borders (including between allies). • Denied licenses cap market growth; compliance failures bring reputational damage and legal liability.	Export-control exposure shapes which markets are reachable and how fast	Early, Growth	• Which of your products require export-control licenses, under which regimes? • In which geographies have you secured, or are you pursuing, export opportunities – and where do you expect license friction? • How would a license denial in a key market change your revenue plan? • Who manages export-control compliance and classification internally?"
2.4 END-USE MONITORING (EUM)	• EUM is legally mandated in many jurisdictions; without it, technology can be diverted to unauthorised, prohibited or hostile users. • Gaps create legal liability, IP loss and human-rights exposure.	Credible EUM protects the company's licences and IP and signals maturity – reducing the diversion tail-risk that weighs on defence-sector valuations.	Growth	• What is the intended end-use of the product, and where are the realistic diversion pathways? • How is your End-Use Monitoring system designed to meet origin-country requirements, and how do you detect misuse post-sale? • What contractual and technical controls (e.g. usage logging, geofencing) support monitoring? • Who owns EUM compliance and how are incidents escalated?"

Theme 3: Security

In defence, trust is not an abstract concept. It shows up in the cap table, in the workforce, in the supplier base, in data systems, and in physical facilities. A technically excellent company can still find itself shut out of the defence market if the ecosystem around it is not trustworthy. Foreign ownership, control, and influence (FOCI) can determine whether a company can access certain contract opportunities. Cybersecurity and data-security practices can determine whether a company is viewed as a credible partner and eligible to bid for contracts. Personnel security and facility-clearance issues can decide which revenue opportunities are actually reachable and whether the company is vulnerable to security breaches by adversaries, IP theft, or worse.

CATEGORY	WHY IT MATTERS & ASSOCIATED RISKS	CONTEXT & BUSINESS CASE	FUNDING STAGE	DUE DILIGENCE QUESTIONS
3.1 FOREIGN OWNERSHIP, CONTROL & INFLUENCE (FOCI)	• Undisclosed or unmanaged foreign ownership/ control can trigger loss of contract eligibility, forced mitigation agreements, or exclusion from classified work. • Adversarial influence risks sabotage, IP theft and counterintelligence exposure.	FOCI status is often a hard gate for defence contracts and clearances.	All	• How is your current cap table composed? • Which contracts or clearances require FOCI mitigation, and what mitigation instruments (voting trusts, proxy agreements, SSA) would apply? • Who monitors and reports changes in beneficial ownership?
3.2 TRUSTED CAPITAL	• Adversarial or opaque capital on the cap table can enable sabotage, IP theft or counter-intelligence access, and can disqualify a company from sensitive programmes.	Trusted capital' screening protects the company's core market and makes it a cleaner asset for later investors and acquirers.	All	• How do you verify that your capital sources are 'trusted', and which screening tools do you use? • Do you have any current or prospective exposure to adversarial or opaque capital, and how are you managing it? • How do you diligence co-investors before accepting them onto the cap table?"
3.3 TRUSTED WORKFORCE	• Personnel with access to classified or sensitive tech who are under detrimental foreign influence create security and clearance risk.	Clearance-eligible leadership and staff are a prerequisite for classified revenue. Nationality mix and clearance readiness directly affect which contracts are reachable.	All	• Do you anticipate clearance challenges for any executives or key staff, and why? • What clearance levels does your product or customer set require? • What personnel security controls (foreign-contact reporting, technology control plans) do you have?
3.4 TRUSTED SUPPLIERS	• Compromised suppliers create sabotage, IP-theft and supply-disruption risk, and can breach customer FOCI requirements. • Dependencies on one supplier can result in supply chain shortage	Supplier trust protects continuity of critical inputs and contract compliance	Early, Growth	• How do you diligence and monitor suppliers in line with national laws and customer requirements? • Have you experienced or do you suspect any sabotage, tampering or adversarial influence in your chain? • How do you assure second sources for security-critical components?
3.5 TRUSTED DATA / DATA SECURITY	• Cyberattacks and breaches at defence companies commonly lead to IP theft and compromise of national-security information. • Non-compliance with customer data-security standards breaches vendor and supply-chain contracts.	Data-security compliance (e.g. CMMC / DFARS, NIST) is increasingly a contract prerequisite.	Early, Growth	• What data will you collect / store, and how is it classified (if at all)? • Which mandatory data-security standards must you meet for your target customers, and where are you in that compliance journey? • Which voluntary standards (NIST CSF, ISO 27001) are you adopting, and why? • Who owns data-security compliance and how is it resourced?
3.6 PHYSICAL SECURITY	• Dealing with defence and national security can put the physical safety of team and facilities at risk and must appropiately be addressed.	Facility clearance is often required to perform classified work – a prerequisite for a whole class of contracts and therefore for the associated revenue.	Early, Growth	• What physical security protocols do you have for your facilities and personel? • Who owns facility-clearance and security compliance internally?

Theme 4: Governance & Compliance

Defence contracts are often high-value, government-linked, and politically sensitive, which makes anti-bribery and corruption controls especially important. Because rules, norms, sanctions regimes, and defence customer requirements are continually evolving, investors should also ask whether the team is actively tracking and engaging with the regulatory landscape—or waiting to be surprised by it.

CATEGORY	WHY IT MATTERS & ASSOCIATED RISKS	CONTEXT & BUSINESS CASE	FUNDING STAGE	DUE DILIGENCE QUESTIONS
4.1 CORPORATE GOVERNANCE & ANTI-BRIBERY/CORRUPTION	• High-value, government-tied contracts create acute bribery/corruption exposure; violations bring severe legal, financial and reputational damage.	Strong governance and ABC controls protect contract eligibility and reduce legal tail-risk	Growth	• What is your governance structure and board oversight of safety, security, and responsible use? • Do you have a formal Anti-Bribery & Corruption policy, a designated compliance owner reporting to the board, and annual training for at-risk roles? • How are incidents documented, escalated and remediated, and have their been incidents to date? "
4.2 INTERNATIONAL LAW & HUMAN RIGHTS DUE DILIGENCE (HRDD)	• Products developed/sold without regard to IHL and human-rights standards risk enabling misuse, civilian harm and complicity in violations and is required to sell to governments. • Absence of HRDD creates legal, reputational and financing exposure (esp. with LPs and DFIs).	A credible HRDD system reduces the misuse tail-risk that most weighs on defence-sector reputations and access to capital.	Growth	• Do you conduct (or plan) human-rights due diligence / impact assessments, and for which deployment geographies? • How does your 'red-flag' / no-sale system work – what criteria and indices define it, and who decides? • What safeguards prevent use of your technology in violation of IHL / IHRL? • What monitoring, remedy and grievance mechanisms exist when harm is alleged?"
4.3 LEGAL & REGULATORY UNCERTAINTY	• Emerging-tech defence companies face fast-shifting geopolitics, rules and norms on standards, applications and safeguarding. • Failing to anticipate change causes costly redesigns, lost contracts and compliance breaches.	Regulatory trajectory is a key swing factor in the investment case. Teams that track and shape policy de-risk the roadmap and can turn new rules into competitive advantage.	All	• Which pending or emerging laws, rules or norms could affect your product, market access or business model? • How are you monitoring and preparing for these (e.g. design standards, export changes, sanctions)? • Are you engaging in standards-setting or policy formation, directly or via associations?"

Theme 5: Operations & Environment

Defence technologies, particularly those involved in operations in extreme conditions (undersea, space, remote & off-grid locations) can have unique climate risk exposures. Technologies that represent novel forms of lethal or destructive force - such as directed energy and electromagnetic warfare - can have distinct impacts on health and safety and ecological and biosphere that must be evaluated.

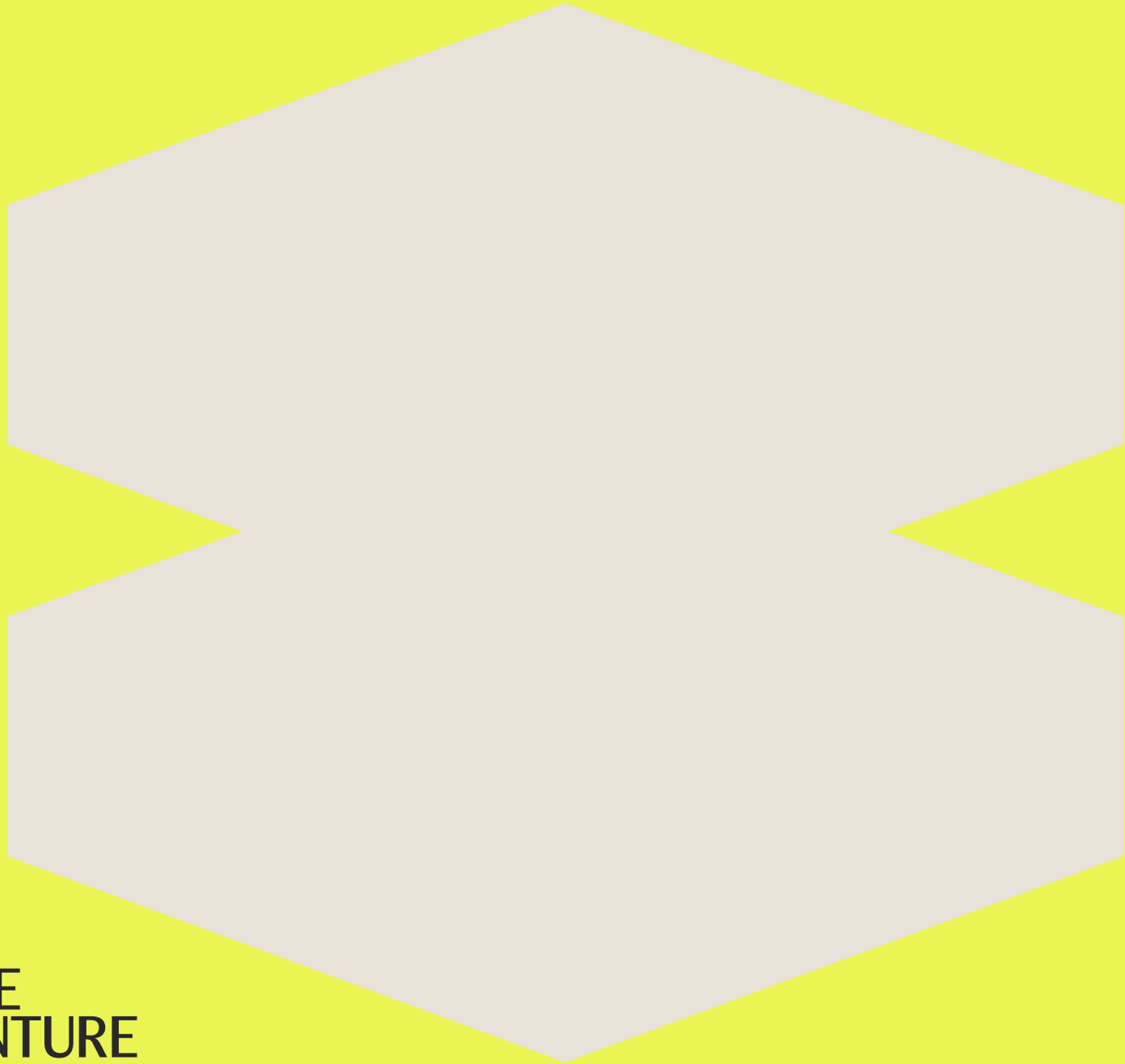
CATEGORY	WHY IT MATTERS & ASSOCIATED RISKS	CONTEXT & BUSINESS CASE	FUNDING STAGE	DUE DILIGENCE QUESTIONS
5.1 HEALTH & SAFETY	• Unsafe lab, R&D or manufacturing environments risk accidents, injuries or fatalities and regulatory non-compliance. • Inadequate protocols for hazardous materials or advanced equipment threaten operational continuity and customer trust.	Strong H&S underpins operational continuity and is a marker of overall operational discipline that customers and acquirers read across to quality and reliability.	Early, Growth	• What H&S incidents have occurred in the past 12 months, and how were they handled and prevented from recurring? • How do you monitor compliance with H&S regulations, and who owns oversight? • What protocols and training are in place for hazardous materials and advanced equipment?
5.2 ENVIRONMENTAL FOOTPRINT OF OPERATIONS	• High energy/compute intensity, water use, hazardous materials and waste create rising costs, regulatory exposure and reputational risk.	Resource intensity is both a cost driver and a compliance risk as energy/water/waste rules tighten. Tracking it early avoids retrofits and supports customer sustainability requirements.	Early, Growth	• How do you track energy, water and emissions across R&D, compute and manufacturing, and how will these scale? • Where do you see resource use as a cost or regulatory risk as you grow, and how are you mitigating it? • How do you manage hazardous materials and waste, and who is responsible?
5.3 CLIMATE RISKS	• Fcilities / suppliers exposed to extreme weather face downtime, cost spikes, insurance gaps and delayed R&D.	Climate exposure affects continuity, insurability and cost base Products designed for a changing operating environment also open opportunity.	Growth	• Where are your facilities and critical suppliers, and how exposed are they to extreme-weather and biodiversity-related risk? • Have you assessed physical climate vulnerabilities, and how could climate events affect your ability to scale? • How could emerging climate regulation (carbon pricing, mandates) affect operations or market access?

Theme 6: AI & Autonomy

While AI & Autonomy are not applicable to all defence sectors, it is becoming the foundation for many defence applications and where some of the most material risks lie. This section is designed to guide the safety of AI applications and to ensure alignment with international law. The risks in this section strongly affect product function and the ability to deliver capability, and are therefore more technical in nature.

CATEGORY	WHY IT MATTERS & ASSOCIATED RISKS	CONTEXT & BUSINESS CASE	FUNDING STAGE	DUE DILIGENCE QUESTIONS
6.1 HUMAN CONTROL & ACCOUNTABILITY	• AI-assisted engagement or navigation without clear human control can cause misidentification, unintended engagement and unlawful harm. • Undefined responsibility leaves the company and operators exposed when systems act unpredictably.	Demonstrable human control and clear accountability are becoming procurement and legal prerequisites (e.g. DoDD 3000.09). They are central to whether a system is buyable by responsible customers.	All	• Where exactly does human judgment end and machine decision-making begin, and what is the required level of human judgment to select/engage targets? • How can a human deactivate, override or intervene, and can they do so within realistic time constraints? • If the system acts unpredictably, who is the identified responsible party, and how are manufacturer vs. operator responsibilities defined in your and your customers' policies? • How does the design comply with distinction, proportionality and military-necessity principles?
6.2 TARGET IDENTIFICATION & BIAS	• False positives/negatives and biased training data or recognition systems can cause civilian harm and misidentification • Unmitigated bias is a legal, ethical and reputational liability.	Bias and target-ID performance are critical for successful product development and delivery	All	• How do you mitigate false positives/negatives in target identification, and what safeguards prevent civilian harm? • How do you test for and reduce bias in models and data, including adversarial and edge cases? • What datasets are used and how is data quality assured?
6.3 RELIABILITY & SAFETY ENVELOPE (TEVV)	• Undefined operational limits and testing only in ideal conditions lead to unsafe deployment and failure to validate the safety case.	Rigorous Test, Evaluation, Verification & Validation (TEVV) in realistic conditions is what lets a system pass customer acceptance and field trials	Early, Growth	• What are the defined environmental and operational limits of the system, and what happens at the edges? • How does your TEVV plan reflect realistic and adversarial conditions (EW, GNSS-denied, degraded comms, weather) rather than lab-perfect scenarios? • What independent validation, certification or third-party testing are you pursuing? • How do you track measures of effectiveness/performance and feed failures back into design (e.g. a FRACAS-type loop)?
6.4 EXPLAINABILITY & TRACEABILITY	• If operators/auditors cannot understand system behaviour, unlawful or unsafe outcomes cannot be detected, explained or corrected. • Poor traceability blocks incident investigation and accountability.	Explainability and audit trails build the customer trust needed for adoption.	Early, Growth	• Can the system explain its target-identification or decision process to a commander in operationally meaningful terms? • What mission logs, model/data lineage and audit trails do you maintain, and how would they support an incident investigation? • How do you keep explanations meaningful as models evolve?

6.5 CONNECTIVITY, FAIL-SAFE & ADVERSARIAL RESILIENCE	• Loss of datalink can cause uncontrolled or unsafe behaviour and inability to abort/recall. • Susceptibility to jamming, spoofing or cyber manipulation can be exploited by adversaries.	The operating environment is changing rapidly, product and product testing needs to be able to adapt quickly	Early, Growth	• What happens if the system loses comms – how does it safely disengage, and can you show abort/recall/return-to-base functioning in practice? • How does it operate and stay safe in GPS/GNSS-denied environments? • What EW/cyber red-team testing have you done, and what changed as a result?
6.6 DATA & MODEL SECURITY	• Model/data manipulation, theft or capture can compromise performance, IP and national security. • Captured platforms can leak sensitive data or models.	Securing models and data protects the core asset and meets customer security requirements	Early, Growth	• How do you secure models, data and algorithms against manipulation and exfiltration? • What happens if a platform is captured – is data/model protected, wiped or rendered unusable? • How do you control access to training data and model weights?
6.7 DESTRUCTIVE FORCE AND & LEGAL WEAPONS REVIEW	• Products with intentional or unintentional potential for lethal/destructive force carry the highest legal and reputational risk. • Governments are starting to require Article-36-style legal review risks for compliance with IHL/IHRL for froniter tech.	For weapons-capable systems, a legal weapons review and IHL-aligned design are gating for lawful sale and for acceptance by customers	Early, Growth	• Does your product have intentional or unintentional potential for lethal or destructive force? Walk me through the scenarios. • Have you conducted or planned an Article-36-style legal weapons review, and what did/will it assess? • How do you ensure compliance with IHL/IHRL through design and use constraints? • Which jurisdictions apply and who owns safety oversight?
6.8 RESPONSIBLE-USE CULTURE & GOVERNANCE	• Leadership that treats responsible use as box-ticking, with no designated lead or escalation paths, is a risk Weak product-level oversight compounds every risk above.	Leadership mindset are among the strongest predictors of whether risks are managed – a key qualitative signal for investors and a driver of long-term reputation.	All	• Who owns Responsible Use in your company, and what authority and board visibility do they have? • How are incidents documented and escalated, and what role does the board play in overseeing such risks? • What responsibility do you feel for how your technology is ultimately used?



REFRAME
VENTURE