

End-user and end-use screening: a practical guide for modern export compliance, including military end-use insights



Christopher Salmon
Chief Executive



This article explores the role of end-user and end-use screening in modern export compliance. We explain how verifying *who* receives your products and *what* they intend to do protects against diversion, sanctions breaches, and dual-use violations. Military end-use vectors receive particular attention, highlighting the high-risk stakes. Gain insights into building a robust screening programme, closing common governance gaps, and transforming screening from a regulatory necessity into a strategic advantage for operations across complex global supply chains.

In modern global trade, knowing *who* is buying your goods is just as important as knowing *what* they will do with them.

For many traders, that distinction – between **end-user** and **end-use** – sits at the heart of effective export controls compliance. In short, an “*end-user*” is the entity taking possession of the product or asset, while “*end-use*” relates to the intended application of that product or asset, whether civilian, commercial, or – more complicated in nature – sensitive military purposes.

Regulators are paying closer attention than ever. Unchecked transfers can result in diversion to prohibited parties, violation of dual-use goods export controls, or inadvertent breaches of sanctions regimes. For multinational boardrooms and senior strategists, this is

not dismissable as technical box-ticking: a failure in your end-user and end-use screening programme has the potential to jeopardise market access, commercial success, reputational standing, and regulatory trust... in addition to creating opportunities for serious national security breaches.

As well as mitigating the risk of penalties, a robust internal compliance programme signals to partners, customers, and regulators that your organisation truly understands the geopolitical risks that can sit within trade operations, and takes proactive steps to safeguard against them. This is why – with dual-use technology, sensitive goods, and complex supply chains – screening has become a boardroom-level imperative.

Why this matters

Effective end-user and end-use screening protects your business from regulatory, operational, and reputational risks. Multinational firms that integrate these checks strategically can anticipate diversion, safeguard market access, and navigate high-risk military or dual-use transactions with confidence; turning a compliance requirement into a competitive advantage across global trade operations.

➤ **Borders for the Boardroom:**
Christopher Salmon on
supply chain resilience



Listen now on Spotify
and Apple Music

Core principles of screening

End-user screening: *knowing your customer*

End-user screening starts with verifying the identity and legitimacy of your buyers. This would include:

- Confirming the entity's legal registration
- Any beneficial ownership
- Ensuring they are not listed on any denied party or restricted lists

In order to handle this efficiently, international firms increasingly rely on digital databases, third-party verification services, and automated tools to make these checks both thorough and scalable.

Jurisdictional frameworks vary, so 360° awareness is crucial. For instance, the U.S. EAR outlines specific end-user obligations, while the [UK Export Control Order](#) and [EU Dual-Use Regulation](#) impose parallel (but not necessarily identical) requirements. A sound grasp of these differences allows companies to structure a compliance programme that is defensible across multiple jurisdictions, and thereby reduce the risk of inadvertent violations.

End-user screening: *understanding their intent*

While knowing your customer is essential, understanding the intended application of your goods – **end-use** verification – is equally important. Specifically, companies must assess whether distributed products/assets *could* be used in military, nuclear, or other sensitive sectors. Red flags include attempts to divert technology, opaque supply chains, or participation in high-risk industries.

Strategically, end-use screening protects market access and ensures regulatory compliance – preventing costly border seizures or license revocations. By documenting the intended use and conducting periodic reviews, businesses create a robust audit trail that demonstrates proactive risk management and the capability to accurately assess export control risk.



What is military end use screening?

Military end use screening is a specialised layer of end-use checks, focusing on items that have the capacity to be applied in defense or armed forces contexts.

Beyond conventional dual-use considerations, this involves analysing whether a product might be incorporated into military hardware, weapon systems, or technologies that could have national security implications. Companies must implement structured processes to comply with military end-use controls, including obtaining explicit declarations, reviewing supply chain touchpoints, and verifying customers' operational profile. Integrating these steps ensures high-risk transfers are flagged early; helping protect global market access and mitigate potential sanctions exposure.

Why military end use is more heavily regulated

Unlike “ordinary” and purely commercial goods, technologies with potential military application sit on a geopolitical fissure. More than just products, they represent *capabilities*; when they move across borders, they can shift military balance, weaken sanctions, or quietly empower actors that regulators are actively trying to constrain. That is why military end-use screening is treated as a matter of national security, not trade administration.

Items that frequently trigger military-end-use scrutiny include:

- Advanced semiconductors and micro-electronics
- Encrypted communications and networking equipment
- Sensors, radar, and imaging systems
- Navigation, positioning, and guidance technologies
- Aerospace, drone, and unmanned-system components
- Materials and software with weapons, surveillance, or battlefield applications

Frameworks such as the Wassenaar Arrangement exist because once these capabilities escape from approved or intended channels, they are practically impossible to pull back. For boardrooms, the major risk is in becoming part of a security failure that regulators, partners, and markets will not easily forgive.

Practical steps for assessing military end use

Military end-use screening is about understanding how commercial technology can migrate into strategic capability. This is where export compliance becomes a question of governance, risk appetite, and geopolitical exposure.

A mature programme treats military end-use assessment as a decision framework; not a form.

Risk lens	What to ask	Why it matters
Customer identity	<i>Is the buyer, beneficial owner, or end user connected to armed forces, defence ministries, or military-linked contractors?</i>	Many military procurement routes are indirect, using commercial or civilian front entities.
Intended application	<i>Is the product going into aerospace, surveillance, telecoms, energy, advanced manufacturing, or security infrastructure?</i>	These sectors are possible pathways into military programmes.
Technical capability	<i>Could the item enhance targeting, communications, navigation, monitoring, or weapons systems – even if sold as civilian?</i>	Dual-use risk is driven by what technology can do, not how it is marketed.
Geography	<i>Is the destination country subject to arms embargoes, defence controls, or elevated security scrutiny?</i>	Military diversion risk rises sharply in sensitive regions.
Transaction behaviour	<i>Are there unusual shipping routes, intermediaries, or urgency around delivery?</i>	These are classic indicators of diversion or concealment.

Common governance gaps

Even within a well-functioning global supply chain, without careful oversight, controlled technology can travel farther, faster, and more invisibly than ever. **Misaligned supplier due diligence** or gaps in downstream end-use verification can silently erode compliance integrity.

Recordkeeping is another common blind spot: incomplete documentation opens the possibility for audit failures. Moreover, the **digital aspect** of modern trade further complicates matters – SaaS solutions, cloud platforms, and virtual product access can cross borders in ways that traditional compliance frameworks may struggle to capture.

Another layer is added by collaborative R&D and **joint ventures**. When proprietary technology moves between entities, even for testing or development, it can constitute a controlled transfer. Third-party distributors, complex international logistics, and multiple layers of subcontractors increase the risk that items will reach unintended end users

How to build an end-user and end-use screening programme

The most successful international traders treat screening as an integrated part of their export compliance programme, linking legal, operational, and risk-management functions across jurisdictions. The goal is to prevent diversion, reduce regulatory friction, and anticipate high-risk vectors (particularly military end use) before goods or technology leave the facility.

Therefore, a modern programme balances technology, process, and human judgment. Boardrooms can use a strategic checklist to ensure robustness:

- Map **all products and services** subject to dual-use and military end-use controls.
- Maintain up-to-date **denied party and sanctions lists** across all jurisdictions.
- Verify **beneficial ownership** of customers and intermediaries.
- Document **declarations of intended end use** and conduct **pre-shipment checks**.
- Integrate **ongoing monitoring**, audits, and horizon scanning for regulatory changes.
- Embed **escalation protocols** for high-risk or ambiguous transactions.
- Train teams across sourcing, sales, legal, and logistics on end-use **risk awareness**.

Screening is strategic. Not administrative

Ultimately, end-user and end-use screening is best understood as the lens through which multinational firms can interpret their market access, supply chain integrity, and global reputation. Each verification exercise, documented declaration, and pre-shipment review represents legal diligence, yes, but more importantly, a signal to partners, regulators, and markets that your company operates with transparency and control.

Strategic screening also helps mitigate the very highest-risk exposures. Organisations that detect and manage these risks early reduce the likelihood of border delays, serious enforcement actions, or reputational fallout.

End-user and end-use checks must be embedded into enterprise-level governance – not siloed within operations or legal teams. Cross-functional alignment ensures that sourcing, R&D, IT, and logistics decisions are informed by compliance realities, while proactive monitoring and horizon scanning help anticipate regulatory shifts. In this way, screening turns from an operational headache into a source of competitive advantage. Companies that master it move faster, trade more confidently, and safeguard both revenue and reputation: creating a strategic lever for sustainable global growth.



Get in touch: info@clearborder | [clearBorder.co.uk](https://clearborder.co.uk)