

OLYDEFENCE Compliance & Responsible Transfer Brief

A public framework for lawful trade, responsible decisions, product evidence and secure data

Document code	OLYD-PUB-CRB-001	Version / effective date	3.0 / 2 August 2026
Classification	Public / business review	Document owner	OLYDEFENCE — OLYVENRA LTD
Language	English	Status	Publication-ready / controlled master
Purpose			
This brief describes a risk-based governance model. It is not legal advice and does not replace transaction-specific review by competent counsel or authorities.			

Transaction gate

- Identify and verify every material party, beneficial owner, country, route, consignee, final end user and intended end use.
- Classify the goods, software, technology, services and technical information under the laws and control lists applicable to each jurisdiction.
- Assign responsibility for export, import, transit, brokering, firearms, dangerous-goods, medical-device, PPE or other licences and permits.
- Screen sanctions, embargoes, debarment, ownership/control, diversion indicators, suspicious payment arrangements and adverse information.

Responsible-transfer decision

Review the risk that a proposed transfer could contribute to serious violations of international humanitarian law or human rights, unlawful internal repression, terrorism, organised crime, destabilisation or unauthorised re-transfer.

Apply proportionate due diligence, documented mitigation, escalation and refusal/exit criteria. A commercial opportunity does not override a legal, ethical or responsible-transfer concern.

Ammunition and traceability

Ammunition requires through-life records covering manufacturer/designation, lot or batch, production and acceptance data, packaging, dangerous-goods classification, transport, secure storage, shelf life, inspection/surveillance, accountability, incident response and disposal.

Marking and recordkeeping support traceability and anti-diversion. Details are matched to the applicable legal and customer framework; public pages do not disclose sensitive stock or routing information.

Protection, clothing and medical kits

Ballistic, respiratory and other protective claims must relate to the complete exact configuration, test basis, limitations, fit, care and service-life controls. A product-family name or component class alone is insufficient.

Tactical clothing and footwear are specified by user, climate, task, materials, size curve, care and contractually applicable protective performance. First-aid and trauma-kit contents follow the authorised customer's protocol, user training and destination rules; public scope excludes medicines.

Secure information

Classified and export-controlled technical information is not accepted through the public form or ordinary email. Release is limited to authorised persons, countries, systems and purposes, with retention, onward-disclosure, return and destruction controls.

Continuous review

Sanctions, licences, standards, product configurations and official guidance change. Each decision uses current official sources and current product evidence at the relevant transaction stage.

Eight gates before a controlled requirement can progress.

The following evidence is requested proportionately to product risk, destination, customer and transaction stage. OLYDEFENCE does not claim licences, certifications or approvals that have not been verified for the exact scope.

- 1. Legal identity & authority** - Legal name, registration, beneficial ownership, public authority or mandate, authorised signatory and procurement route.
- 2. Parties, destination & sanctions** - Buyer, consignee, end user, intermediaries, countries, transit route, ownership/control and applicable sanctions or embargo checks.
- 3. End use & anti-diversion** - Documented intended use, final location, custody, storage, no unauthorised re-transfer and escalation of diversion indicators.
- 4. Classification & licensing** - Military, dual-use, firearms, dangerous-goods, medical-device, PPE or other classification and the responsible licence holders.
- 5. Product identity & evidence** - Legal manufacturer, model/configuration, part number, serial or lot, current specifications, reports, certificates, labels and instructions.
- 6. Quality & configuration control** - Quality-system scope, inspection/acceptance plan, nonconformance, change notification, authorised substitution and record retention.
- 7. Logistics & lifecycle** - Packaging, transport, storage, shelf/service life, spares, calibration, training, maintenance, warranty, recall and disposal.
- 8. Human rights, IHL & secure data** - Risk-based human-rights/IHL review, responsible business conduct, need-to-know access and protection of controlled technical information.

Official reference framework

Primary official sources used for the public governance framework. Their current text and transaction-specific law always prevail.

- [United Nations - Global Framework for Through-life Conventional Ammunition Management](#)
- [United Nations Office for Disarmament Affairs - Small arms and light weapons](#)
- [UNODA - Marking and recordkeeping](#)
- [European Union - Common Position 2008/944/CFSP, consolidated text](#)
- [International Committee of the Red Cross - Arms transfers](#)
- [OHCHR - UN Guiding Principles on Business and Human Rights](#)
- [UK Export Control Joint Unit - Export controls on military goods, software and technology](#)
- [US BIS - End-user and end-use controls](#)
- [UNECE - UN Model Regulations on the Transport of Dangerous Goods, Rev. 24](#)
- [US National Institute of Justice - Ballistic Resistance of Body Armor, NIJ Standard 0101.07](#)
- [European Union - Regulation \(EU\) 2016/425 on personal protective equipment](#)
- [European Union - Regulation \(EU\) 2017/745 on medical devices](#)
- [World Health Organization - Emergency health kits](#)
- [NATO Support and Procurement Agency - NATO Codification System](#)
- [NIST - Protecting Controlled Unclassified Information, SP 800-171 Rev. 3](#)
- [United Nations Security Council - Consolidated sanctions list](#)

Do not send classified, export-controlled, operationally sensitive or personal medical information through the public form. Product-specific technical data, pricing, stock, licences, end-user records and contracts are shared only after due diligence through an approved channel.

Portfolio governance: configuration, origin, availability, evidence, licensing, end user, end use and support scope are validated for each authorised requirement before supplier engagement or technical release.