
Handbook

Strategic Trade Controls and Dual-Use Goods

A reference manual for law enforcement officers on export permits, transit documents, import permits, detection, intelligence-led enforcement, sanctions sources and investigation.

UNODC-WCO Container Control Programme | Edition 1.0 | October 2026

General reference material, not legal advice. Confirm all legal points against your national law and the current official lists.

Contents

About this handbook	5
The core routine in one page	5
Chapter 1: Foundations of strategic trade control	7
What is strategic trade control?	7
Dual-use goods: same item, two uses	7
Why it matters: the threats we control against	8
Four types of goods you will meet	8
The control toolkit	8
Who does what	9
Key terms (1): how goods move	9
Key terms (2): parties and concepts	9
Chapter 2: The international framework	11
UN Security Council Resolution 1540	11
The export control regimes	11
Treaties behind the controls	12
Sanctions and embargoes	12
From regime lists to national lists	12
Reading a control list: categories and groups	13
Classification: the tariff code is not enough	13
Chapter 3: Legal frameworks: the EU model and your national law	15
EU Regulation (EU) 2021/821 at a glance	15
Scope: which activities are controlled?	15
Catch-all clauses: non-listed items	16
Types of export authorisation	16
Union general export authorisations: EU001 to EU008	16
How authorities decide: licence criteria	17
Penalties and enforcement under EU law	17
Beyond the EU: other major systems	18
Worksheet: your national legal framework	18
Chapter 4: Export permits: what to check and why	20
Does this export need a permit?	20
What an export authorisation application contains	20
End-user certificates and end-use statements	20

Anatomy of an export authorisation: what to check	21
At the border: export verification step by step	21
Declarations, balances and partial shipments	22
Common export violations and tactics	22
Software and technology: the invisible export	23

Chapter 5: Transit and transshipment 24

Transit, transshipment and re-export	24
Why transit hubs are exploited	24
Legal bases for controlling transit	25
Transit and transport documents	25
Checking a transit consignment	25
Port and container risk: where PCCP fits	26
Red flags in transit and transshipment	26
Case study: the BBC China interdiction (2003)	27

Chapter 6: Import permits and certificates 28

Why import controls matter	28
What typically needs an import permit?	28
Import certificates and delivery verification	29
Checking an import permit at the border	29
Import violations and red flags	29

Chapter 7: Detection, risk indicators and safe handling 31

From tariff code to technical data	31
Commonly diverted dual-use commodities	31
Red flags: the customer and the deal	32
Red flags: documents and declarations	32
Risk management and targeting	33
Inspection and safe handling	33

Chapter 8: Intelligence-led enforcement 34

From data to intelligence	34
The intelligence cycle applied to strategic trade	34
Collection sources for strategic trade cases	34
Grading and confidence: the 5x5x5 approach	35
Intelligence versus evidence	35
Sharing, handling and legal principles	36
Tasking, coordination and intelligence products	36

Chapter 9: Sanctions and authoritative sources	38
Why sanctions matter for strategic trade	38
The Global Sanctions Source Registry	38
What the registry contains	38
Core sources for export control and enforcement	39
Using sources safely: a quick routine	40
Limits and caveats of the registry	40
Chapter 10: Investigation, evidence and cooperation	41
Diversion typologies	41
Following the money	41
Investigation toolkit and open-source research	41
Scenario A (fictional): the machine-tool container	42
Scenario B (fictional): the transit truck	42
Scenario C (fictional): the chemical import	43
Evidence and documentation	43
Measures and penalties	43
International cooperation	44
Working with industry	44
Chapter 11: Practical exercises and wrap-up	46
Exercise 1: spot the differences (fictional)	46
Exercise 2: classification walk-through	46
Exercise 3: tabletop at the port	46
Officer's pocket checklist	46
Knowledge check	47
Key takeaways	47
Resources and further reading	48
Annex A: Document checklists	49
Export authorisation	49
End-user statement or certificate	49
Transit or transshipment documents	49
Import permit or certificate	49
Annex B: Red-flag matrix	50
Annex C: Glossary	51
Annex D: Official sources	52

About this handbook

This handbook accompanies the course Strategic Trade Controls and Dual-Use Goods. It can be read on its own. Each chapter opens with a short overview, then covers the topic in sections, with tables and checklists where they help. The annexes at the end contain a one-page decision routine, document checklists, a red-flag matrix, a glossary and a list of official sources.

A note on scope. Strategic trade controls are national law. The handbook uses the European Union system as a worked example and refers to international regimes, but your powers, offences and procedures are set by your own legislation. Fictional case scenarios use invented names and countries. Control lists change at least yearly; always use the current official version.

The core routine in one page

Step	Check	What to ask
1	Identify the item	What is it? Technical data, not the label. Compare with the current control list.
2	Identify the parties	Exporter, consignee, end-user, intermediaries, bank, carrier. Screen against sanctions and restricted-party lists.
3	Check the destination and route	Embargo? Weak-control hub? Transit or transshipment points that make no commercial sense?
4	Check the end-use	Does the end-user's business match the goods? Is there a catch-all concern?
5	Check the authority	Is a licence, permit or certificate required? Genuine, valid, in scope, conditions met?
6	Compare documents with goods	Description, quantity, parties, dates, serial numbers, markings.
7	Decide and record	Release, detain or refer. Notes, photographs, chain of custody. Alert the licensing authority and partners.

Chapter 1: Foundations of strategic trade control

Strategic trade control is the system by which States decide who may move sensitive goods, software and technology across borders, and under what conditions. This chapter sets out the vocabulary and the logic of the system. Its central idea is that risk lies not in the item alone but in the combination of item, party, destination and end-use. A machine tool sold to a furniture factory is ordinary trade; the same machine delivered through three intermediaries to a missile programme is a serious offence. Officers do not need to be engineers, but they must understand why a licence exists, what it proves and what it does not prove.

In this chapter: What strategic trade control is; Dual-use goods and why they matter; Categories of controlled goods; The control toolkit; Who does what; Key terms

What is strategic trade control?

- Government control over items that could help build weapons of mass destruction, missiles or military capability
- Covers goods, software, technology and the services around them
- Applies to export, re-export, transit, transshipment, brokering and import
- Balances security and legitimate trade: most shipments are lawful
- Enforced where trade becomes physical: ports, airports and borders

Side panel: Security without stopping legitimate trade

Strategic trade controls are the legal and administrative system States use to decide which sensitive items may leave, cross or enter their territory, and under what conditions. The word strategic points to the national security purpose. Controls reach beyond physical goods to software, technical data and services such as brokering and technical assistance. Most companies trading in these items are legitimate, so the system is built around licensing and compliance rather than outright bans. Law enforcement matters because a control on paper only works if someone checks the shipment at the border and investigates when the paperwork is false.

Dual-use goods: same item, two uses

Item	Civil use	Misuse concern
Carbon-fibre materials	Aircraft, sports equipment, wind turbines	Rocket motor cases, centrifuge rotors
Precision machine tools	Car and aircraft parts	Weapon and missile components
Industrial chemicals	Plastics, pesticides, medicines	Precursors of chemical warfare agents
Specialised valves and pumps	Chemical and food plants	Nuclear and chemical processing
Drones and components	Survey, farming, filming	Military unmanned aircraft
Advanced electronics	Computing, telecoms, cars	Weapons, radar and surveillance

A dual-use item has legitimate civil applications and can also contribute to weapons of mass destruction, missiles or conventional military systems. What makes an item controlled is its technical specification, such as strength, precision or material, and the context of the sale. This is why officers cannot rely on appearance alone and why the classification step in Chapter 7 matters so much.

Why it matters: the threats we control against

- **Nuclear weapons:** Enrichment and reactor-related equipment, materials and know-how.
- **Chemical and biological:** Precursor chemicals, reactors, fermenters and agents.
- **Missiles and drones:** Propulsion, guidance and composite materials.
- **Conventional arms:** Military goods and parts feeding conflicts and destabilising build-ups.
- **Repression technology:** Surveillance and intrusion tools used against human rights.
- **Sanctions evasion:** Controlled goods routed through third countries to banned users.

Introduce the six risk areas. Nuclear, chemical and biological weapons are the original focus of the multilateral regimes. Missile delivery systems and unmanned aircraft are covered by their own regime. Conventional arms and military technology are covered in parallel by arms export controls. Newer concerns include surveillance and intrusion technology that can be used for internal repression, and the use of third countries to evade sanctions. The point for officers is that the risk is not abstract: diverted components have ended up in weapons programmes.

Four types of goods you will meet

Type	Examples	Typical control
Military items	Weapons, ammunition, military electronics	Arms export licence, national military list
Listed dual-use items	Items in the control list (EU Annex I)	Dual-use export authorisation
Non-listed items of concern	Ordinary goods for a WMD or embargoed military end-use	Authorisation if the authority informs the exporter or the exporter is aware
Sanctioned goods	Items banned to a country or party by a sanctions regime	Prohibition, or licence under the sanctions rules

Officers often confuse these categories. Military items are controlled under arms export law and a separate military list. Listed dual-use items appear in the control list that implements the multilateral regimes; in the EU this is Annex I of Regulation (EU) 2021/821. Non-listed items can still need authorisation through catch-all clauses when the end-use is a concern: for example, an ordinary pump destined for a chemical weapons programme. A single shipment can fall under more than one category, so always check each layer.

The control toolkit

- **Control lists:** Define which items, software and technology are controlled.
- **Licensing:** Authorisation before export, transit, brokering or transfer.
- **End-use and end-user checks:** Who receives the goods and what they will do with them.
- **Catch-all controls:** Authorisation for non-listed items when the end-use is a concern.
- **Services controls:** Brokering, technical assistance and intangible transfers.
- **Enforcement and penalties:** Inspection, detention, investigation, prosecution.

These six tools work together. Control lists say what is controlled. Licensing gives the State a decision point before a transfer happens. End-use and end-user checks reduce the chance that licensed goods are diverted. Catch-all controls close the gap for items that are not on a list but are headed for a worrying use. Controls on brokering, technical assistance and intangible transfers prevent the system being bypassed by moving services or data instead of goods. Enforcement is the backstop, and it is the part officers deliver.

Who does what

Actor	Role in strategic trade control
Licensing authority	Assesses applications, issues permits, gives classification advice
Customs	Checks declarations and goods, runs risk analysis, detains and refers
Police and prosecutors	Investigate and prosecute offences, secure evidence
Intelligence services	Provide threat and end-user information
Technical experts	Confirm classification and advise on safe handling
Industry	Classifies goods, applies for permits, runs compliance programmes
Carriers and forwarders	Hold shipping data and are often first to see anomalies

Make clear that strategic trade control is a team effort. The licensing authority is usually a ministry of economy, trade or foreign affairs, not customs, and officers should know who it is and how to reach it quickly. Customs is the main frontline agency but needs the licensing authority to confirm whether a permit exists and the technical experts to confirm classification. Police and prosecutors take over when an offence is suspected. Intelligence services often supply the tip-offs that lead to seizures. Industry and logistics providers are partners: their compliance staff and shipping data are an important source of early warning.

Key terms (1): how goods move

Term	Meaning
Export	Goods, software or technology leave the territory (or the customs union)
Re-export	Goods that arrived from abroad are sent onward to another destination
Transit	Goods pass through a State on the way to another State, under customs control
Transshipment	Goods are moved from one vessel or aircraft to another at a hub
Import	Goods enter the territory for use or for further customs procedures
Intra-EU transfer	Movement between EU Member States; controlled for the most sensitive items

These terms are used loosely in daily conversation but have specific meanings in law and the differences matter for permits. Export and import are the familiar pair. Re-export becomes important when goods are imported, stored, and then sent on to a different destination than the one first declared. Transit means passage through a territory; transshipment means the physical change of vessel or aircraft, often in a hub port. Intra-EU transfers are normally free of dual-use licensing, but the most sensitive items on Annex IV need authorisation even inside the Union. Check how your national law defines these terms.

Key terms (2): parties and concepts

Term	Meaning
Exporter	Person or company that holds the contract and decides to send the goods
Consignee	Party named in transport documents to receive the goods
End-user	Party that finally uses the goods; may differ from the consignee
End-use	The purpose for which the goods will be used
Broker	Person who arranges a deal between parties without owning the goods
Catch-all	Control on non-listed items when the end-use is a concern
Intangible transfer	Software or technology sent by email, cloud or other electronic means

The consignee and the end-user are frequently different parties, and this is where diversion often hides: a trading company or freight forwarder may be named as consignee while the real end-user is elsewhere. A broker may never touch the goods, yet brokering can be controlled. Catch-all is a policy device: the item is not on any list, but the authority can require a licence if it is, or may be, intended for a prohibited use. Intangible transfers matter because modern technology moves as data.

Chapter 2: The international framework

National controls are not invented in isolation. They implement binding obligations of the United Nations Security Council, treaties such as the Non-Proliferation Treaty, the Chemical Weapons Convention and the Biological Weapons Convention, and politically agreed guidelines of the export control regimes. This chapter explains where the rules come from, how regime lists become national lists, and why officers must always work from the current version of the list. It also explains why a customs tariff code is a pointer and never a substitute for the technical control-list entry.

In this chapter: UN Security Council Resolution 1540; The export control regimes; Treaties behind the controls; Sanctions and embargoes; From regime lists to national lists; Reading a control list; Classification

UN Security Council Resolution 1540

- Adopted in April 2004 under Chapter VII: binding on all States
- Bars support to non-State actors seeking nuclear, chemical or biological weapons and their delivery systems
- Requires effective export, transit, transshipment and brokering controls
- Requires border controls, law enforcement and physical protection of sensitive materials
- The 1540 Committee supports implementation and assistance requests

Callout: 1540 - The legal anchor for national export, transit and transshipment controls

Resolution 1540 is the single most important global legal basis for strategic trade controls because it binds every UN member State, whether or not it takes part in any export control regime. It was adopted on 28 April 2004 under Chapter VII of the UN Charter. It obliges States to refrain from supporting non-State actors that try to acquire nuclear, chemical or biological weapons and their means of delivery, to criminalise such activity, and to put in place effective domestic controls. The controls it names include export, transit, transshipment and re-export controls and controls on brokering, plus border controls and law enforcement effort. For officers the message is simple: your border controls are part of an international obligation, and your State can ask for training and equipment support.

The export control regimes

Regime	Since	Focus	Main list
Wassenaar Arrangement	1996	Conventional arms; dual-use goods and technology	Munitions List; Dual-Use List
Nuclear Suppliers Group	1975	Nuclear items and nuclear-related dual-use	Guidelines, Parts 1 and 2
Missile Technology Control Regime	1987	Missiles and unmanned aircraft able to deliver WMD	MTCR Annex
Australia Group	1985	Chemical and biological weapons precursors, equipment, agents	Common control lists
Zangger Committee	1971	Nuclear exports under the NPT	Trigger List

Key point: Politically binding, consensus-based and implemented through national law.

They are not treaties: participating governments commit politically to apply common standards through their national laws. The Wassenaar Arrangement covers conventional arms and dual-use items and was established in 1996. The Missile Technology Control Regime, from 1987, covers missiles and unmanned aerial vehicles. The Zangger Committee, from 1971, interprets the nuclear export obligations of the Non-Proliferation Treaty and maintains a Trigger List. Membership numbers change, so check the websites listed at the end of the course. Regime decisions each year become amendments to national control lists.

Treaties behind the controls

- **Non-Proliferation Treaty:** 1968. Nuclear safeguards under the IAEA and restraint on nuclear exports.
- **Chemical Weapons Convention:** Bans chemical weapons; scheduled chemicals tightly controlled; OPCW verifies.
- **Biological Weapons Convention:** 1972. Bans biological and toxin weapons; no verification body.
- **Arms Trade Treaty:** In force since 2014. Covers export, import, transit, transshipment and brokering.
- **UN Firearms Protocol:** 2001. Licensing for firearms export, import and transit.

These treaties create binding obligations that sit behind the national export control laws. The Non-Proliferation Treaty and IAEA safeguards underpin nuclear controls. The Chemical Weapons Convention lists chemicals in three Schedules with progressively lighter controls, and it restricts transfers of scheduled chemicals to States that are not party to it; the OPCW is the implementing body. The Biological Weapons Convention bans biological and toxin weapons but has no formal verification mechanism, which increases the importance of national export controls. The Arms Trade Treaty, adopted in 2013 and in force from December 2014, is the only treaty that explicitly covers transit, transshipment and brokering of conventional arms. The Firearms Protocol to the UN Convention against Transnational Organized Crime requires licensing for the import, export and transit of firearms.

Sanctions and embargoes

- UN Security Council measures are binding on all States
 - The EU, US and others add their own sanctions: goods bans, end-use bans, asset freezes
 - Sanctions can restrict export, import, transit and services, including non-listed items
 - Party lists (people and entities) complement item lists
 - Measures change often: always check the current text
- Side box: Remember** - Item control and party control are different checks; A licence for the item does not clear a sanctioned party; Sanctions may ban goods that no control list covers

Sanctions run in parallel to export control lists. UN Security Council sanctions, such as arms embargoes and measures against specific countries, are binding on every State. The EU and other jurisdictions add autonomous measures that can ban certain goods or services, prohibit specific end-uses, or freeze the assets of listed persons. In practice an officer must carry out two checks: is the item controlled, and is any party or the destination subject to sanctions? A shipment can be perfectly legal under the dual-use rules and still breach a sanctions ban, and the reverse. Because sanctions are updated frequently, officers should use official consolidated lists and internal guidance rather than memory.

From regime lists to national lists

1. **Regime decides:** Plenary meetings agree list changes, usually each year.
2. **Region or State adopts:** In the EU, a Commission delegated act amends Annex I.
3. **Authorities update tools:** Licensing and customs systems, guidance and correlation tables.
4. **Officers apply:** Use the current version and check for updates.

Key point: EU Annex I was last updated by a delegated regulation adopted on 8 September 2025.

This process explains why lists change and why officers must keep their reference material up to date. In the EU the Commission adopts a delegated regulation amending Annex I of Regulation (EU) 2021/821; the update adopted on 8 September 2025 added or changed controls in areas such as quantum technology, semiconductor manufacturing and testing equipment, advanced computing circuits, additive manufacturing and peptide synthesisers. Verify the publication reference and date of application in the Official Journal before you quote it, because the entry into force follows a scrutiny period. Other States have their own procedures, so ask your licensing authority how and when changes reach the border.

Reading a control list: categories and groups

Cat.	Subject
0	Nuclear materials and equipment
1	Special materials and equipment
2	Materials processing
3	Electronics
4	Computers
5	Telecoms and information security
6	Sensors and lasers
7	Navigation and avionics
8	Marine
9	Aerospace and propulsion
Group	Type of entry
A	Systems, equipment and components
B	Test, inspection and production equipment
C	Materials
D	Software
E	Technology

Entries contain technical parameters, so classification often needs a data sheet. Other control lists, such as the Wassenaar Dual-Use List, use a similar structure, which makes it easier to compare systems.

Classification: the tariff code is not enough

- Tariff (HS/CN) codes describe what an item is; control lists describe what it can do
- One tariff code can hold both controlled and non-controlled items
- Correlation tables point to likely entries: they are not proof
- Real classification needs the technical specification and often expert advice
- Misclassification, accidental or deliberate, is a common route to illegal exports

Callout: HS ≠ control - Always compare the technical data with the control list entry

The two systems do not map neatly onto each other. For example, a machine tool can fall under the same tariff heading whether it is a basic model or a high-precision one that meets a control threshold. Customs correlation tables help to flag which tariff codes may contain controlled goods, but the final answer depends on the technical data sheet. Where the exporter has not provided data, ask the licensing authority or a technical expert for a classification opinion. Wrong tariff codes on a declaration are a red flag in themselves.

Chapter 3: Legal frameworks: the EU model and your national law

The European Union Dual-Use Regulation, Regulation (EU) 2021/821, is used here as a worked example of a complete legal framework because it is detailed, public and widely copied. The chapter then shows how other major systems compare and gives a worksheet to map your own national law. Whatever the system, officers should be able to answer five questions: what is controlled, who must apply for authority, who grants it, what powers officers have, and what the penalties are.

In this chapter: EU Regulation (EU) 2021/821; Scope of the controls; Catch-all clauses; Authorisation types and EU general authorisations; Decision criteria; Penalties and enforcement; Other major systems; Your national framework

EU Regulation (EU) 2021/821 at a glance

- Adopted 20 May 2021, applies since 9 September 2021; recasts Regulation 428/2009
- Directly applicable in all Member States and enforced nationally
- Controls export, brokering, technical assistance, transit and intra-EU transfers
- Annex I lists controlled dual-use items and is updated regularly
- Licensing decisions stay with national competent authorities

Side panel: One EU-wide list, national licensing and enforcement

Regulation (EU) 2021/821 is the current EU legal basis for the control of exports, brokering, technical assistance, transit and transfers of dual-use items. It replaced Regulation (EC) 428/2009 and has applied since 9 September 2021. As a regulation it applies directly in all Member States, but each Member State designates its own competent authority for licensing and sets its own penalties. Annex I is the common control list. The Commission updates Annex I through delegated acts, normally every year, to reflect decisions in the multilateral regimes. National laws add procedures, penalties and powers of customs and police.

Scope: which activities are controlled?

Activity	Rule under the EU Regulation
Export	Authorisation needed for Annex I items leaving the EU customs territory
Re-export	Non-Union items shipped out again are treated as exports
Transit	A Member State may prohibit transit of non-Union items with WMD or embargo concerns
Brokering	Authorisation if the broker is informed or aware of WMD or military end-use concerns
Technical assistance	Member States may prohibit or license it on the same grounds
Intangible transfer	Software and technology sent electronically count as export
Intra-EU transfer	Authorisation needed for the most sensitive items in Annex IV

This table shows that the controls go beyond physical exports. Export covers items leaving the EU customs territory. Re-export is treated like export when non-Union items are shipped out again.

Transit is dealt with in Article 7: a Member State may prohibit the transit of non-Union dual-use items if they are, or may be, intended for weapons of mass destruction or a military end-use in an embargoed country. Brokering and technical assistance controls close loopholes for services. Software and technology sent by email or cloud are exports even though nothing crosses the border physically. Finally, goods circulate freely inside the Union, except the most sensitive items in Annex IV, which need authorisation for intra-EU transfers as well. Always check how your national law fills in the gaps the Regulation leaves to Member States.

Catch-all clauses: non-listed items

- **WMD end-use:** Items intended for the development or production of nuclear, chemical or biological weapons or missiles.
- **Military end-use:** Items for a military end-use in a country under an arms embargo.
- **Parts of military items:** Items used as parts of military goods that were exported illegally.
- **Cyber-surveillance:** Items that may be used for internal repression or serious human rights violations.

Key point: Duty: tell the authority if you know of such an end-use. The authority can then require a licence.

Catch-all controls apply to items that are not on Annex I. Under Article 4, an authorisation is needed when the authority informs the exporter that the items are, or may be, intended for weapons of mass destruction or missile use, for a military end-use in an arms-embargoed country, or as parts of illegally exported military items. Under Article 5, a similar mechanism applies to cyber-surveillance items that may be used for internal repression or serious violations of human rights and international humanitarian law. The exporter has a duty to notify the authority if it is aware of such an end-use. For officers, the practical effect is that a lack of a listing does not close the case: if you have information about a worrying end-use, escalate it so that the licensing authority can inform the exporter and require a licence.

Types of export authorisation

Type	Who and what it covers	Typical use
Individual	One exporter, one end-user, specified items and quantity	One-off deals, higher-risk sales
Global	One exporter, several destinations or end-users, specified items	Regular customers with a track record
National general	Published by a Member State, set conditions and destinations	Routine low-risk trade under national law
Union general	EU001 to EU008, open to registered exporters EU-wide	Low-risk destinations and defined cases

The Regulation provides four forms of export authorisation. An individual authorisation is tied to one exporter, one end-user and a defined quantity. A global authorisation allows one exporter to ship specified items to several destinations or end-users and is usually granted to companies with a good compliance record. A national general authorisation is published by a Member State and open to any exporter that meets the conditions. Union general export authorisations are created by the Regulation itself and apply across the EU. When a company says it holds a general authorisation, ask which one, and check that the shipment fits the conditions.

Union general export authorisations: EU001 to EU008

Code	What it covers
EU001	Most Annex I items to low-risk destinations (e.g. USA, UK, Japan, Canada, Australia, Switzerland)
EU002	Certain electronics and telecoms items to a short list of destinations
EU003	Export after repair or replacement
EU004	Temporary export for exhibitions or fairs, with re-import
EU005	Certain telecommunications items
EU006	Specified chemicals to listed destinations
EU007	Intra-group transfers of software and technology
EU008	Certain encryption items

Key point: Exporters register with the competent authority, declare the code and report use. Check the current text.

The Union general export authorisations remove the need for an individual licence in lower-risk situations, but they come with strict conditions: registration with the competent authority, notification of first use, record keeping, and in some cases annual reporting. The authorisation code must be declared in the customs documents. They never cover the most sensitive Annex IV items, and they cannot be used if the exporter knows or has been informed that the goods are for a prohibited end-use, such as weapons of mass destruction or a military end-use in an embargoed country. The detailed list of destinations and excluded items differs between authorisations and is amended from time to time, so quote the destination list from the current Annex II rather than from memory. When you meet a declared EU001, check the destination and that the item is not excluded.

How authorities decide: licence criteria

- International obligations and regime commitments
- Sanctions and embargo obligations
- National foreign and security policy, including the EU Common Position on arms exports
- Intended end-use and the risk of diversion
- Exporter's compliance record and internal compliance programme

Side box: Why officers care - Licence conditions can restrict re-export; Refused or withdrawn licences are intelligence; Share suspicious findings with the authority

Article 15 of the Regulation lists what Member States must consider when deciding on an application: their obligations under the regimes and treaties, their obligations under sanctions, considerations of national foreign and security policy, including those covered by the Common Position on arms exports, and considerations about the intended end-use and the risk of diversion. Authorities also look at the exporter's compliance record. Officers do not make the licence decision, but they benefit from understanding it. Licence conditions, such as no re-export without consent or delivery verification, are what officers may need to check later. Refused or revoked applications and information from the authority can be strong risk indicators for targeting.

Penalties and enforcement under EU law

- Member States must set effective, proportionate and dissuasive penalties
- Typical measures: administrative fines, imprisonment, confiscation, licence withdrawal
- Directive (EU) 2024/1226 harmonises criminal offences for breaches of EU sanctions
- Competent authorities cooperate and exchange information across Member States
- Exporters must keep detailed records; retention periods are set in law

Side panel: Penalties are national: know your own offences and powers

The Regulation requires each Member State to lay down penalties, but it does not harmonise them for dual-use offences, so maximum fines and prison terms differ widely. Directive (EU) 2024/1226 harmonises criminal offences and penalties for violating EU restrictive measures, which can overlap with dual-use violations when goods are sanctioned; Member States had to transpose it by May 2025, so check the status in your Member State. The Regulation also provides for administrative cooperation and information exchange between competent authorities and with customs. Exporters have record-keeping duties that officers can use to audit a company after a stop.

Beyond the EU: other major systems

System	Main instruments	Features worth knowing
United States	Export Administration Regulations (EAR); ITAR for military items	Broad reach over US-origin items wherever they are; denied-party lists
United Kingdom	Export Control Order 2008 and related trade controls	Own control list; licensing by a dedicated unit; trade and transit controls
Japan	Foreign Exchange and Foreign Trade Act	List controls plus catch-all
China	Export Control Law (2020)	Control lists, licensing and end-user management
India	SCOMET list under foreign trade law	Licensing for listed items and technology

The United States applies the Export Administration Regulations to dual-use and less sensitive military items and the International Traffic in Arms Regulations to defence items; US rules can follow US-origin goods and technology after they leave the United States, which affects re-exports. The United Kingdom has its own control list and trade controls. Japan, China and India each have national laws with their own control lists and catch-all provisions. Do not present this as a legal summary: laws change and the detail is complex. The purpose is to show why exporters sometimes need several licences for the same shipment, and why information sharing between enforcement agencies is valuable.

Worksheet: your national legal framework

Question	Your country: fill in
Which authority issues strategic trade licences?	
Which control list is in force, and where is it published?	
Which law lets you stop, inspect, detain or seize goods?	
Is there a transit or transshipment control?	
Which offences and penalties apply?	
Who gives technical classification advice?	

Collect the completed worksheets and keep them as a reference for follow-up work and for building the contact list used in Chapter 8.

Chapter 4: Export permits: what to check and why

Export is the stage at which most controls are applied and where the licensing authority has most information. This chapter follows the exporter's decision process, the content of an application, the end-user statement, the checks an officer makes at the border, and the typical violations. Officers verify that the authorisation is genuine, valid and matches the shipment; they do not re-take the licensing decision.

In this chapter: When a permit is needed; What an application contains; End-user certificates; Anatomy of an authorisation; Verification at the border; Declarations and balances; Common violations; Software and technology

Does this export need a permit?

1. **Classify:** Is the item, software or technology on a control list?
2. **Check destination:** Embargo, sanctions or low-risk destination?
3. **Check end-use and end-user:** Catch-all concerns? Sanctioned or suspicious parties?
4. **Choose authorisation:** Individual, global, national or Union general.
5. **Apply and wait:** No shipment before the decision and conditions are met.

Key point: A responsible exporter follows these five steps. Officers verify that the paperwork matches reality.

This is the exporter's decision path, which officers should understand so they can test whether a company has actually followed it. Step one is classification: the exporter must determine whether the item is on the control list, using the technical data. Step two checks the destination against embargoes, sanctions and general authorisation eligibility. Step three looks at the end-user and the end-use, including catch-all concerns and denied-party lists. Step four selects the right type of authorisation, and step five is the application. Goods must not leave until the authorisation is granted and its conditions can be met. When you stop a shipment, ask the exporter to explain how they classified the item and where the authorisation came from; vague answers are themselves a risk indicator.

What an export authorisation application contains

- **Parties:** Exporter, consignee and end-user names and addresses.
- **End-use:** What the goods will be used for and where.
- **Items:** Description, control list entry and technical specification.
- **Quantity and value:** How many units and the contract value.
- **Route:** Destination and any transit or transshipment countries.
- **Supporting documents:** Contract, invoice, end-user certificate, import certificate.

An application gives the licensing authority what it needs to assess the risk. The parties section identifies the exporter, the consignee and the end-user: these may be three different organisations. The end-use statement says what the goods are for. The item description and technical specification link the goods to a control list entry. Quantity and value allow the authority to cap the licence and later to check shipments against it. Route information matters for transit and transshipment checks. Supporting documents such as the contract, invoice, end-user certificate and sometimes an import certificate from the destination State let the authority test the claims. Officers can ask for copies of these documents when a shipment looks suspicious.

End-user certificates and end-use statements

- A signed statement of the final user, the end-use and the commitment not to re-export without consent
- Typical content: items, quantity, end-user identity and address, place of use, signature, date
- Some importing States issue official certificates; others accept company statements
- Verify the signatory's authority, letterhead, seals and consistency with the order
- Forged or altered certificates are a primary diversion tool

Side box: Check - Does the end-user's business match the goods?; Is the signatory real and authorised?; Does the address exist?; Is the certificate used more than once?

An end-user certificate is the main assurance given to an exporting State that goods will reach the stated user and be used for the stated purpose. A good certificate names the end-user, describes the goods and quantity, states the place and purpose of use, and contains an undertaking not to re-export or transfer without consent. Importing States may issue official certificates or endorse company statements. Because the certificate is the exporter's key evidence, it is also a favourite target for forgery. Officers should check that the signatory exists and has authority, that the letterhead and seal are genuine, that the address exists, and that the end-user's business plausibly needs the goods. If in doubt, contact the issuing authority directly using official contact details, not those printed on the document.

Anatomy of an export authorisation: what to check

Field	What the officer checks
Number and issuing authority	Genuine reference; authority is the competent one
Validity dates	Shipment falls inside the validity period
Exporter	Matches the export declaration
Consignee and end-user	Match the transport documents and invoice
Item and control entry	Goods match the description and classification
Quantity and value	Within the authorised balance
Destination	Matches declared destination and route
Conditions	Endorsements, re-export limits, delivery verification
Signature and security features	Stamps, signatures and paper match specimens

Each row is a verification point. The number and issuing authority must be genuine: if possible, verify through the licensing authority's system or hotline. Validity dates are often the first thing to go wrong; shipments sometimes leave after a licence has expired. The exporter, consignee and end-user must match the declaration and the commercial documents; a changed name or address is a red flag. The item description and classification must match the goods you see. Quantity and value are checked against the licence balance, since licences are drawn down as partial shipments leave. Destination and route should be consistent. Conditions can include delivery verification or limits on re-export. Finally, check the security features against specimens where available.

At the border: export verification step by step

1. **Declaration:** Get the export declaration and the authorisation reference.
2. **Documents:** Compare authorisation, invoice, packing list and transport document.
3. **Goods:** Match description, quantity and markings to the papers.
4. **Classification:** Does the item fit a listed entry? Call an expert if unsure.
5. **Decision:** Release, deduct quantity, detain or refer.
6. **Record:** Endorse, copy documents and report.

This six-step routine can be applied at any border post, port or airport. Start with the export declaration, which should contain the authorisation reference where one is required. Then compare the documents against each other: the authorisation, commercial invoice, packing list and transport document must be consistent about parties, goods, quantity and destination. Next, look at the goods themselves. If the physical goods differ from the paperwork, that is the key finding. If the classification is uncertain, do not guess: call the licensing authority or a technical expert. Decide whether to release, deduct from the licence balance, detain or refer for investigation. Record the outcome, keep copies, and report according to your agency's procedure so that information flows to the licensing authority and to risk analysts.

Declarations, balances and partial shipments

- The authorisation reference must appear in the export declaration
- General authorisations are declared by their code (for example EU001)
- Partial shipments are deducted from the authorised quantity and value
- A mismatch between declaration and authorisation means: stop and verify
- Electronic links between licensing and customs systems reduce paper fraud

Side panel: Mismatch = stop and verify

Authorisations only work as a control if shipments are matched to them. The authorisation reference or general authorisation code goes into the export declaration, following your national customs instructions for the data fields. Licences are limited by quantity and value, so each shipment reduces the balance; the exporter or the system must record this. Repeated partial shipments just under a threshold can indicate splitting. Where licensing and customs systems are linked electronically, the system can flag invalid or exhausted licences automatically; where they are not, officers must check manually or by telephone. Any mismatch between the declaration and the authorisation is a reason to stop and verify before release.

Common export violations and tactics

- **Wrong classification:** Item declared as not controlled, often with a vague or generic description.
- **No authorisation:** Exports claimed as spare parts or samples with no permit.
- **False end-user:** Forged or misleading end-user details or destination.
- **Splitting shipments:** Controlled goods sent in small lots across several dates or routes.
- **Undervaluation:** Values too low to attract attention, or unusual prices.
- **Forwarder as consignee:** A freight forwarder or trader named in place of the true end-user.

These are recurring patterns seen in enforcement. Wrong classification can be innocent or deliberate, and vague descriptions such as machine parts or electronic components are a common cover. Some exporters simply do not apply for a permit, claiming that the goods are spare parts or samples. False end-users and false destinations are typical in diversion cases. Splitting shipments aims to avoid scrutiny or to stay under thresholds. Undervaluation reduces duties and lowers risk scores. A freight forwarder or trading company named as consignee can hide the real end-user.

Software and technology: the invisible export

- Controls cover software and technology, not only physical goods
- Email, cloud sharing, remote access and even meetings can be an export
- Officers rarely see the transfer: evidence is on devices and servers
- Look for laptops, drives, drawings and design files with business travellers
- Involve the licensing authority and digital forensics early

Side panel: Data moves faster than cargo

This is called an intangible transfer. It is difficult for frontline officers to detect, so they should focus on opportunities they do see: business travellers carrying laptops, drives and printed drawings, or companies that send engineers to install and train. Where an investigation starts, digital forensics will be essential to find the evidence. Work with the licensing authority early because classification of software and technology often needs expert input.

Chapter 5: Transit and transshipment

Transit and transshipment are the area where controls are weakest and where law enforcement can add the most value. Goods in transit are often not declared as exports or imports in the transit State, and diversion networks deliberately route shipments through the State with the lightest controls. This chapter covers the legal basis for transit controls, the documents that accompany transit movements, how to check a consignment, and a historic case that shows how a transit hub was used to disguise a proliferation network.

In this chapter: Transit, transshipment and re-export; Why hubs are exploited; Legal bases for transit controls; Transit and transport documents; Checking a consignment; Port and container risk; Red flags; Case study

Transit, transshipment and re-export

Term	Meaning	Example
Transit	Goods cross a State on the way to another State under customs control	A truck from A to C crossing B
Transshipment	Goods move from one vessel or aircraft to another at a hub	Feeder to mother vessel at a port
Re-export	Imported goods are sent on to another destination	Goods stored after import, then sent to a third State
Free zone	Area with special customs rules for storage and processing	Repacking and relabelling before onward shipment

Make sure everyone uses the same words. Transit is passage through a territory, usually under a customs transit procedure and guarantee. Transshipment is the physical transfer between vessels or aircraft, typically at a hub port or airport, and the goods usually remain under customs supervision. Re-export means goods that were imported are sent on to another destination, often after storage or a customs procedure. Free zones and bonded warehouses allow storage, repacking and sometimes processing with limited customs formalities, which can be abused to change labels, documents or even the apparent origin.

Why transit hubs are exploited

- Hub ports handle huge volumes: only a small share of containers can be inspected
- Goods may be "just passing" and never declared as import or export
- Consignee and final destination can change while goods are in transit
- Free zones and warehouses allow repacking, relabelling and new documents
- Controls differ between States: criminals choose the weakest link

Callout: Weakest link - Diversion networks route goods through the State with the lightest controls

Illicit procurement networks use transit and transshipment for three reasons. First, volume: major hubs move millions of containers and cannot inspect more than a fraction. Second, legal gaps: goods in transit are often outside licensing and declaration systems, especially if the transit State has no transit control. Third, flexibility: documents, consignees and destinations can be changed while the goods are on their way, and free zones allow repacking and relabelling. Criminals pick routes through States with weaker controls or less capacity. This is why international cooperation and risk-based targeting are so important: no single State can close the gap alone, and a hub State that does control transit protects other countries too.

Legal bases for controlling transit

- UNSCR 1540 calls for controls over transshipment of nuclear, chemical and biological items
- Arms Trade Treaty and the Firearms Protocol address transit and transshipment of arms
- EU: a Member State may prohibit transit of non-Union dual-use items with WMD or embargo risk
- National law may require a transit licence or notification, or allow detention and re-routing
- Sanctions regimes often ban transit or transshipment of listed goods

Side box: Ask yourself - Do I have a legal power to stop goods in transit?; Who must I notify?; Which State can I alert?

Several layers of law apply to transit. Resolution 1540 requires controls on transit and transshipment of items related to nuclear, chemical and biological weapons and their delivery systems. The Arms Trade Treaty requires States to take appropriate measures to regulate transit and transshipment of conventional arms where necessary and feasible, and the Firearms Protocol includes provisions on transit shipments. In the EU, Article 7 of the dual-use Regulation lets a Member State prohibit transit of non-Union dual-use items if they are or may be intended for weapons of mass destruction or for military end-use in an embargoed country. National legislation may go further by requiring a transit licence or notification or by giving customs the power to detain and re-route goods. Sanctions regimes often prohibit transit of listed goods. The key question for each officer is whether they have a clear legal power to act, and whom they must inform.

Transit and transport documents

Document	What it tells you
Transit declaration (T1/T2 in the EU)	Route, goods, customs guarantee, office of destination
Bill of lading (sea)	Shipper, consignee, notify party, ports, container and seal numbers
Air waybill (air)	Shipper, consignee, flights, destination, description
Cargo manifest / entry summary	What the carrier declared before arrival
Commercial invoice and packing list	Description, quantity, value, parties
Transit authorisation, if required	Permission to pass through
End-user certificate, origin certificate	Final use and origin of the goods

Officers checking a transit consignment should compare as many documents as possible. The transit declaration, such as T1 or T2 in the EU's transit system, shows the route and the guarantee. The bill of lading or air waybill is the transport contract and names the shipper, consignee and often a notify party. The manifest or entry summary shows what the carrier declared to customs. The commercial invoice and packing list give the description, quantity and value. A transit authorisation may be required in some States. An end-user certificate or certificate of origin gives further context. Inconsistencies between documents, such as different weights, descriptions or parties, are red flags. Request missing documents rather than assume everything is in order.

Checking a transit consignment

1. **Identify:** Container, seal, bill of lading and waybill numbers.
2. **Compare:** Declaration, manifest and transport papers against each other.
3. **Assess:** Goods, route, parties and red flags together.
4. **Decide:** Release, request documents, inspect, detain or refer.
5. **Inform:** Alert partner customs and the licensing authority; record.

This routine is designed for ports and border crossings with limited time. Identification starts with the container number, seal numbers and the bill of lading or waybill number so that every document and message refers to the same consignment. Then compare the declaration with the manifest and the transport documents. Assess the goods, route and parties as a whole rather than looking for a single red flag. Decide on the proportionate action: release, ask for more documents, inspect, detain or refer. Finally inform the partners: customs in the country of origin and destination, and the licensing authority. A shipment that you release without informing others may be diverted later in the chain, so information sharing is part of the job, not an optional extra.

Port and container risk: where PCCP fits

- UNODC-WCO Container Control Programme sets up port control units that profile and target containers
- Add strategic trade indicators to targeting: parties, commodity, route, history
- Combine manifest data, carrier information and previous detections
- Use WCO secure channels (CENcomm, ContainerComm) to share alerts quickly
- Alert both the country of origin and the country of destination

Side panel: Risk profiling and information sharing close the transit gap

The UNODC-WCO Container Control Programme helps States to build specialised units at seaports, dry ports and airports that use risk analysis to target high-risk containers and cargo. Strategic trade enforcement fits naturally: the same targeting units can add dual-use and proliferation indicators to their profiles, and can use the same secure communication channels to alert partners. Useful data sources include manifest and entry summary data, information from carriers and forwarders, routing, previous detections and intelligence. The WCO provides secure messaging, such as CENcomm and ContainerComm, and the Customs Enforcement Network database for sharing information about seizures. The WCO also runs a Strategic Trade Control Enforcement programme with guidance for customs. Remember to alert both ends of the route, because the origin State may be able to act on the exporter and the destination State on the importer.

Red flags in transit and transshipment

Route and logistics

- Routing is unusual for the stated origin and destination
- Destination changes after departure
- Several hubs with no commercial reason
- Container opened, repacked or re-sealed in a free zone
- Shipment passes a weak-control State near a high-risk destination

Documents and parties

- Consignee "to order" with unknown notify party
- Generic description such as "machine parts"
- Forwarder named as final consignee
- Inconsistent details between bill of lading, invoice and manifest
- Shipper and consignee unrelated to the goods' sector

Present red flags as indicators, not proof. Route and logistics flags include routes that make no commercial sense, such as a long detour through a hub, destination changes after the goods have left, repeated transshipment, and opening or repacking of containers in free zones. Document and party flags include consignee to order with an unknown notify party, vague descriptions, forwarders listed as final consignee, and inconsistent documents. No single flag should trigger a seizure, but two or three together justify closer inspection and an alert to partners.

Case study: the BBC China interdiction (2003)

- Centrifuge components for uranium enrichment were made in Malaysia and sent to Dubai
- There they were transshipped onto the BBC China, bound for Libya
- Intelligence cooperation led to the ship being redirected to Taranto, Italy, in October 2003
- Inspection revealed a procurement network using front companies and several countries
- The case contributed to Libya's decision in December 2003 to abandon its WMD programmes

Side box: Lessons - Components made in one State, shipped via another; Transshipment hides the real destination; Cooperation across agencies and States works

This is a publicly reported case that shows how transshipment and front companies can be used for proliferation and how interdiction works when intelligence and customs cooperate. Components for gas centrifuges were produced in a third country, shipped to a transshipment hub, and loaded onto the vessel BBC China bound for Libya. Following intelligence cooperation, the vessel was redirected to Taranto in Italy in October 2003, where the containers were inspected. The seizure provided evidence of the wider supply network linked to A.Q. Khan, and it formed part of the events that led Libya to announce in December 2003 that it would give up its weapons of mass destruction programmes. The lessons for officers are that diversion networks exploit several jurisdictions, that hubs are used to obscure the route, and that early information sharing makes interdiction possible.

Chapter 6: Import permits and certificates

Import controls are often less developed than export controls, but they are the other half of a legitimate transfer chain: exporting States ask for proof that the importing State accepts the transfer, and importing States need to know what enters their territory. This chapter covers what needs an import permit, import and delivery verification certificates, how to check a permit, and the violations and red flags that suggest a false or misused import document.

In this chapter: Why import controls matter; What needs an import permit; Import certificates and delivery verification; Checking an import permit; Violations and red flags

Why import controls matter

- Exporting States often require proof that the importing State agrees to the transfer
- Import controls stop sensitive items entering without oversight
- They create documents that can be cross-checked with the exporter's licence
- Import authorisation is the other half of a legitimate transfer chain
- Weak import controls make a State a target for diversion and re-export

Side panel: Two States, two permits: export and import must match

Import controls matter for several reasons. Exporting States, especially for firearms, ammunition, explosives and some chemicals, ask for an import permit or certificate from the destination State before they issue an export licence. That gives the exporting State assurance that the transfer is known and approved. Import controls also stop dangerous items entering the country without oversight, such as firearms, explosives precursors, scheduled chemicals and radioactive sources. They produce documents that can be cross-checked against the exporter's licence. Finally, States with weak import controls can become targets for diversion: goods enter, are re-exported or redirected, and the lack of controls makes tracing difficult. Link this to UNSCR 1540 and the Firearms Protocol.

What typically needs an import permit?

Category	Typical import control	Basis
Firearms, parts, ammunition	Import authorisation for each consignment	Firearms Protocol; Arms Trade Treaty
Explosives and precursors	Licence or registration of import and use	National and regional law
Scheduled chemicals	Restricted or banned from non-parties; declarations	Chemical Weapons Convention
Nuclear and radioactive materials	Authorisation by the regulatory body	IAEA guidance; national law
Military goods	Import licence in many States	National law
Drug precursors	Authorisation or notification	1988 UN Convention
Sanctioned goods	Import bans or licensing	UN, EU and other sanctions

This table gives examples of categories that commonly need an import permit, but the details differ by State. Firearms and ammunition almost always need import authorisation, supported by the Firearms Protocol and the Arms Trade Treaty. Explosives and their precursors are subject to licensing, registration or restrictions, for example under EU rules on explosives precursors. Under

the Chemical Weapons Convention, imports of scheduled chemicals from States that are not party to it are restricted, and States must make declarations. Nuclear and radioactive materials usually need authorisation by a regulatory body and follow IAEA guidance. Many States license imports of military goods. Drug precursors fall under the 1988 UN Convention. Sanctions can ban imports of listed goods or from listed origins.

Import certificates and delivery verification

1. **Importer applies:** For an import permit or certificate from the importing State.
2. **Import certificate:** Authority issues it and states it knows of the transfer.
3. **Export licence:** Exporting State relies on the certificate before licensing.
4. **Shipment and clearance:** Goods are shipped and cleared against the permit.
5. **Delivery verification:** Importer confirms receipt; the confirmation returns to the exporting State.

Some transfers use a documented chain of assurance. The importer applies to its own authority for an import permit or certificate, sometimes called an international import certificate. The importing authority issues it and thereby confirms that it is aware of the transfer. The exporting State relies on this certificate when it grants the export licence. After shipment and clearance, the importer provides delivery verification, often called a delivery verification certificate, confirming that the goods arrived. The confirmation goes back to the exporting State. For officers, the chain provides cross-check points: does the certificate match the shipment, and is delivery verification missing for earlier shipments? Missing or repeatedly late delivery verification is a diversion indicator.

Checking an import permit at the border

- Is the permit valid, for this importer and for these goods?
- Do consignor, origin and consignment details match the shipping documents?
- Is the importer registered or licensed for this category?
- Are quantities within the permit balance, and are partial shipments recorded?
- Check conditions on storage, end-use and onward transfer; verify authenticity with the issuer

Side panel: Match the permit to the importer, the goods and the paperwork

Checking an import permit follows the same logic as an export check. Validate the permit itself: dates, number, issuing authority and security features. Confirm that the permit names the importer that is presenting the goods and covers these specific goods and this quantity. Compare the consignor and the country of origin with the transport documents. Check whether the importer is authorised for the category, such as a licensed firearms dealer or a registered chemicals importer. Confirm that quantities are within the permit and record partial shipments. Look for conditions, such as secure storage or limits on onward transfer. When you doubt the authenticity of the permit, verify with the issuing authority through official contact details. Remember that an import permit is not a licence to trade in controlled goods in general.

Import violations and red flags

- **Permit and goods differ:** Different goods, quantity or consignor than the permit shows.
- **Forged or altered permit:** Altered text, doubtful stamps or numbers that cannot be verified.
- **Importer not authorised:** New or shell importer not registered for the category.
- **Mislabelled goods:** Controlled goods declared as ordinary commodities.
- **Import for re-export:** Goods imported and quickly sent on without authorisation.
- **No delivery verification:** Repeated shipments with no confirmation of receipt.

Typical import violations are mirror images of export violations. The permit and the goods do not match: different quantity, different substance, different consignor. Permits may be forged or altered; look for inconsistent fonts and stamps, numbers that do not exist in the authority's system, or copies that are not originals. The importer may be a new company or a shell without registration for the category. Controlled goods may be mislabelled as ordinary commodities, particularly chemicals and electronic components. Some importers bring goods in only to re-export them quickly to another destination without authorisation. Repeated shipments without delivery verification are a red flag. Use these as prompts for risk profiles and for follow-up questions to importers.

Chapter 7: Detection, risk indicators and safe handling

Detection turns knowledge into practice. This chapter shows how to move from a tariff code to technical data, which commodities are most often diverted, the red flags in the customer, the deal and the documents, how risk management and targeting work, and how to inspect and handle unknown equipment safely. A red flag is a reason to ask questions, not proof of an offence.

In this chapter: From tariff code to technical data; Commonly diverted commodities; Red flags: customer and deal; Red flags: documents; Risk management and targeting; Inspection and safe handling

From tariff code to technical data

1. **Read the description:** Is it vague, generic or unusual for this trader?
2. **Use the correlation table:** Which control list entries could match this tariff code?
3. **Get technical data:** Manufacturer, model, data sheet and specifications.
4. **Compare parameters:** Do the specifications meet the entry's parameters?
5. **Ask the expert:** Licensing authority or technical expert confirms in writing.

Key point: No data sheet, no classification: refer, do not guess.

This is the practical classification routine. Start with the goods description on the declaration: vague terms, such as parts, equipment or components, are warning signs. Use the correlation table between tariff codes and control list entries to see which entries might apply. Request technical documentation: manufacturer, model, data sheet and specifications. Compare the parameters against the entry; the thresholds are in the control list. If you cannot tell, ask the licensing authority or a technical expert for a written opinion, which also helps as evidence later. Do not try to settle borderline classification yourself. If the exporter cannot or will not provide technical data, that is an indicator in itself.

Commonly diverted dual-use commodities

Sector	Examples of controlled items	Concern
Nuclear-related	Vacuum equipment, frequency changers, specialised valves, high-strength materials	Enrichment and reactor programmes
Missiles and drones	Composite materials, inertial navigation, small engines, flight controls	Missile and UAV production
Chemical and biological	Precursor chemicals, reactors, fermenters, filters	Chemical and biological weapons
Electronics	Advanced chips, programmable logic, test equipment	Military end-use, sanctions evasion
Machine tools	Multi-axis CNC machines, measuring equipment	Weapon and missile parts
Information technology	Intrusion and surveillance tools, encryption	Repression and cyber operations

These categories reflect public descriptions of the kinds of items that proliferation networks and sanctions evaders seek. Nuclear-related items include vacuum equipment, frequency changers, specialised valves and high-strength materials. Missile and drone programmes need composite materials, navigation components and small engines. Chemical and biological programmes use

precursor chemicals and process equipment such as reactors and fermenters. Advanced electronics are high on sanctions evaders' shopping lists because of their military uses. Machine tools can make weapon parts. Information technology covers intrusion and surveillance tools. The list is not exhaustive and does not give thresholds; the exact parameters are in the control lists. Use the table to prompt local discussion: what moves through your port or airport, and what would worry you?

Red flags: the customer and the deal

Customer behaviour

- Reluctant to give end-use information
- Business does not fit the product
- Lacks the technical background for the item
- Declines installation, training or maintenance
- New company, residential or P.O. box address

Deal structure

- Cash or third-party payment
- Unusually favourable terms or prices
- Quantity inconsistent with normal trade
- Shipping route or packing does not make sense
- Freight forwarder named as final destination

These indicators are drawn from widely published know-your-customer guidance. The customer behaviour column concerns the buyer: refusing to explain what the goods are for, a business that does not match the product, lack of technical knowledge, declining routine services that a genuine buyer would want, and a company with no track record or a doubtful address. The deal structure column covers the transaction: payment that does not fit, terms that are too good to be true, quantities that do not match normal trade, unusual routes or packing, and a freight forwarder as final consignee. Individually these signs may have innocent explanations. Combined, they justify questions, further checks and sharing information with partners.

Red flags: documents and declarations

Indicator	Why it matters
Vague description ("parts", "equipment")	Hides the real item and its control status
Tariff code does not match the goods	Misclassification, accidental or deliberate
Value too low or too high	Undervaluation or trade-based money laundering
Same address for different parties	Front companies and shell structures
Weights or quantities differ between documents	Goods may have been swapped or split
Altered stamps, fonts or signatures	Possible forgery of licences or certificates
Authorisation number cannot be verified	Licence may not exist or may be invalid

Documentary red flags are often the easiest to spot because officers already compare documents routinely. Vague descriptions hide control status. Tariff codes that do not match the goods suggest misclassification. Prices that are far too low or too high may indicate undervaluation or trade-based money laundering. The same address for several parties is typical of shell structures. Weights and quantities that differ between documents suggest goods have been swapped or split. Altered stamps, fonts or signatures point to forgery. An authorisation number that cannot be verified may mean the licence does not exist. Teach officers to record exactly which discrepancy they found, because that is the basis of their reasonable suspicion and later the evidence.

Risk management and targeting

- **Data:** Declarations, manifests, entry summaries, past detections, open sources.
- **Profiles and rules:** Combine parties, commodity, route and history into indicators.
- **Selectivity:** Inspect when several indicators coincide, not for a single flag.
- **Feedback loop:** Feed inspection results back into profiles.
- **Partners:** Link with the licensing authority and foreign customs.

Risk management lets limited inspection capacity find the right shipments. Data comes from declarations, manifests and entry summaries, past detections, open sources and intelligence. Profiles and rules combine several indicators, such as a certain commodity, a certain route and a new importer, because single indicators produce too many false alerts. Selectivity means inspecting when several indicators coincide. A feedback loop ensures that inspection results, positive or negative, update the profiles. Finally, partnerships matter: the licensing authority can confirm quickly whether an exporter holds a licence, and foreign customs can confirm the identity and history of parties. This is where the Container Control Programme's targeting units and information networks are particularly useful.

Inspection and safe handling

- Treat unknown equipment, chemicals and materials as potentially hazardous
- Do not open, test or taste unknown substances; isolate the area and call experts
- Photograph markings, labels, serial numbers and packaging before moving anything
- Sample only with trained staff under a documented chain of custody
- Follow national CBRN and hazardous-materials protocols

Side panel: Your safety first: isolate, record and call the expert

Unknown goods can be dangerous. Chemical, biological, radiological or nuclear materials can harm officers without any visible sign. The rule is: do not open or test unknown containers or substances; isolate the area, keep people away and call trained responders. Document first with photographs of the packaging, markings, labels, serial numbers and the container as found, before anything is moved. Sampling should be done only by trained staff under a documented chain of custody, so that results are valid in court. Follow your national CBRN and hazardous-materials procedures and make sure each officer knows who to call. Practise the emergency contact chain during the course.

Chapter 8: Intelligence-led enforcement

Most diversion cases are found by analysis, not by luck at the border: a pattern across shipments, a front company that appears in three seizures, a payment that does not fit the trade. This chapter applies crime-intelligence methods to strategic trade: the intelligence cycle, collection sources, grading, the difference between intelligence and evidence, sharing and handling, and tasking and products.

In this chapter: From data to intelligence; The intelligence cycle; Collection: open sources and financial data; Grading and confidence; Intelligence versus evidence; Sharing and handling; Tasking and feedback

From data to intelligence

1. **Data:** A raw fact: a declaration line, an HS code, a vessel name.
 2. **Information:** Data put in context: this consignee appears in four declarations.
 3. **Intelligence:** Analysed information that answers a question and supports a decision.
 4. **Action:** Targeting, inspection, referral, investigation or a partner alert.
- Key point: Intelligence is information that has been evaluated, analysed and given meaning for a decision.*

Start with the difference between data, information and intelligence. A single declaration line is data. Seeing that the same consignee has received machine tools through three different freight forwarders is information. Concluding that the consignee is probably a procurement front for a restricted end-user, with a stated confidence and a recommended action, is intelligence. Officers collect a great deal of data every day; the skill is turning it into something a decision maker can use. Also mention the three levels: strategic intelligence informs policy and priorities, operational intelligence supports a specific investigation or operation, and tactical intelligence supports immediate action such as a targeted inspection today. Strategic trade work uses all three.

The intelligence cycle applied to strategic trade

1. **Direction:** Set the question: which routes or traders are most at risk?
 2. **Collection:** Declarations, licences, open sources, financial reports, partner data.
 3. **Evaluation:** Grade the source and the information before using it.
 4. **Analysis:** Link entities, test hypotheses, state confidence.
 5. **Dissemination:** Right product, right people, right handling code.
 6. **Feedback:** Did the alert lead to a result? Refine the next tasking.
- Key point: Most failures happen at direction and feedback, not at collection.*

Direction means a clear intelligence requirement, for example: which transit routes are used to divert machine tools to a sanctioned end-user? Without a question, collection becomes a pile of data. Collection draws on declarations and licence data, open sources, financial intelligence, partner agency data and human sources. Evaluation grades reliability before anything is used. Analysis links people, companies, vessels and addresses, tests alternative explanations and states how confident the analyst is. Dissemination puts the product in front of the people who can act, with the right handling code. Feedback closes the loop: if a risk alert produced no seizures and no learning, the next requirement should change. Common failure points are vague requirements, collecting only what is easy, no evaluation, products that are too long or too late, and no feedback from the user to the analyst.

Collection sources for strategic trade cases

Source type	Strategic trade examples	Main caution
Open source (OSINT)	Company websites, trade fairs, shipping and vessel data, procurement notices	Verify; sites can be false or stale
Financial (FININT)	Suspicious transaction reports, letters of credit, payment chains	Strict access and legal gateways
Customs and licence data	Declarations, licence history, refusals, inspection results	Check data quality and currency
Partner agencies	Licensing authority, police, intelligence service, foreign customs	Respect handling codes
Human sources	Informants, industry tip-offs, whistle-blowers	Protect identity, check motive
Technical	Seized devices, tracking, scans, communications	Lawful authority is essential

These are the main collection disciplines. For strategic trade, open sources are often the fastest way to test a story: does the end-user's website describe a business that needs these goods, is the vessel's history consistent, did the company appear on a procurement notice? Financial intelligence is especially valuable because diversion networks must pay for goods and the payment chain often runs through intermediaries in a third country. Customs and licence data hold the history of the trader and are available to you now. Partner agencies, including the licensing authority, hold refusals and previous concerns that you cannot see otherwise. Human sources and technical collection need lawful authority and specialist handling.

Grading and confidence: the 5x5x5 approach

Element	What is assessed	Typical scale
Source evaluation	How reliable is the source?	A completely reliable to E untested
Information evaluation	How certain is the information?	1 known to be true to 5 suspected to be false
Handling code	Who may see it and why?	1 to 5, from sharing allowed to restricted
Analytic confidence	How sure is the conclusion?	Low, moderate or high, with reasons

Key point: Use your own agency's grading scale. Grade at collection and review when new facts arrive.

Many agencies use the 5x5x5 model: one rating for the source, one for the information, and a handling code. The scales vary between agencies, so always use your own and state which scale you used when you share a product with another service. The key point is that an anonymous tip about a front company is not worthless, but it should not be treated as proven fact either. Add analytic confidence for conclusions, with plain language words such as 'we assess that' and 'it is likely that', and say why confidence is low, moderate or high.

Intelligence versus evidence

Intelligence

- Guides decisions, targeting and priorities
- Can use hearsay and sensitive sources
- Protected by handling codes and sanitisation
- Judged on usefulness and confidence
- Rarely disclosed to the defence

Evidence

- Proves facts to the legal standard in court
- Must be lawfully obtained and admissible
- Subject to disclosure and challenge
- Needs chain of custody and a named witness
- Collected by plan, once a lead is confirmed

Key point: Intelligence starts the case. Evidence wins it.

This distinction protects both sources and prosecutions. A risk alert from a foreign partner may justify holding a container, but the legal case must stand on evidence you collect yourself in a lawful way: the documents, the goods, expert classification, witness statements and financial records. Where intelligence must be used, agencies sanitise it by removing the source, method and sensitive detail before it reaches an investigator or a court, and the original owner must agree. Never tell a suspect or an outside party that you acted on intelligence unless your procedures allow it.

Sharing, handling and legal principles

Share

- Need to know and right to know
- Use agreed channels and gateways
- Include the grading and handling code
- Keep a record of what was shared

Protect

- Originator controls onward sharing
- Never copy codes to open channels
- Protect sources and methods
- Sanitise before wider release

Stay lawful

- Legality: lawful authority for each step
- Necessity and proportionality
- Data protection and human rights
- Accountability and audit trail

Sharing is essential in strategic trade because diversion crosses borders and no single agency sees the whole chain. Share on a need-to-know basis, through agreed channels, with the grading and handling code attached, and keep a record. The originator owns the information: do not pass it on without permission. Protect sources and methods, and sanitise before wider release. Everything must be lawful, necessary and proportionate, comply with data protection rules and human rights standards, and leave an audit trail. Poor handling can end a source's career or life and can end a case. Use the agency channels in your own country and, for international exchange, the secure networks introduced in Chapter 7 such as CENcomm.

Tasking, coordination and intelligence products

-
- **Tasking:** A clear requirement, owner, deadline and feedback route.
 - **Coordination:** Customs, police, licensing and intelligence agree who leads and who shares.
 - **Alerts and risk profiles:** Short, current notices that frontline officers can act on today.
 - **Network and link analysis:** Charts of companies, people, vessels and payments that show who controls whom.
 - **Assessments:** Strategic reports on routes, commodities and trends to set priorities.
 - **Feedback to the source:** Tell the originator what happened, so the next product is better.

Close the module with the products and the coordination that make intelligence useful. A good tasking has a clear requirement, an owner, a deadline and a feedback route. Coordination means customs, police, the licensing authority and the intelligence service agree on who leads and how information flows, ideally in a joint targeting cell. Products range from short alerts and risk profiles for frontline officers, through network charts that show who controls which company, to strategic assessments that set priorities. Always give feedback to the originator: a risk alert that led to a seizure should be reported back so the next one improves.

Chapter 9: Sanctions and authoritative sources

Sanctions and export controls overlap. An item may be uncontrolled on a list yet still prohibited because of the destination, the consignee or the end-use. This chapter explains why sanctions matter, introduces the Global Sanctions Source Registry as a finding aid to official sources, and gives a safe routine for using lists. The registry is a research tool and not a legal authority: always confirm against the official publisher and your national authority.

In this chapter: Why sanctions matter for strategic trade; The Global Sanctions Source Registry; Core sources for officers; Export control, licensing and enforcement pages; Using sources safely; Limits and caveats

Why sanctions matter for strategic trade

- **Embargoes:** Arms and dual-use embargoes ban specific goods to specific destinations, even when no licence list applies.
- **Listed parties:** Asset freezes and trade bans on named persons and entities. A listed party in the chain stops the deal.
- **Evasion methods:** Shell companies, shadow fleets, false vessel data, transshipment hubs and altered documents.

Key point: Check the item, the party, the destination and the route, every time.

Sanctions add three questions to the export-control questions already covered in the course. First, is there an embargo on the destination that prohibits the goods whether or not they are on a control list? Second, is any party in the chain, including banks, shippers and vessel owners, on a sanctions list? Third, does the route or vessel suggest evasion? Typical evasion methods include layered shell companies, ship-to-ship transfers, switched-off tracking, false flag or IMO data, and re-labelling of goods at transshipment hubs. Common high priority items, which are dual-use items found in Russian weapons on the battlefield, are identified by HS code in joint lists by the EU, US, UK and Japan, and are a good example of customs-code level targeting.

The Global Sanctions Source Registry

- A research registry of official sanctions and export-control publishers
- 451 source entries across 230 publishers worldwide
- Covers UN member states, observers, international bodies and 18 additional jurisdictions
- Each entry records the authority, URL, source type, priority and verification status
- 403 entries are official sources verified; 46 are official institutional entry pages only

Callout: 451 - official source entries to find the right page fast

The registry was compiled as a finding aid. Each entry records the publishing jurisdiction, the authority, the source name and URL, a source type, a priority, a verification status, a coverage layer, the regime basis, published formats, topics, region and a research date. There are 451 entries from 230 publishers. The verification field matters: 403 entries are official sources that were verified, 46 are only the official institutional entry page where no specific sanctions page was identified, and a small number are third-party or de facto authority sources and are flagged as such. The 18 additional jurisdictions include territories and administrations that publish their own measures, for example Hong Kong, the Cayman Islands, Jersey, Gibraltar and Taiwan.

What the registry contains

Source type	Entries	Use for officers
Implementation	152	How a State applies sanctions nationally
Lists	103	Names of designated persons and entities
Announcements	61	New measures, amendments and guidance
Institutional entry	46	Official front page when no specific page exists
Legal	24	Laws and regulations
Enforcement	21	Penalties, seizures and case news
Export control	21	Control lists, guidance and end-user rules
Licensing and debarment	14	General licences and debarred firms

Key point: Counts from the registry of 451 entries. Six smaller categories (9 entries) are not shown.

This table shows the main source types. Implementation pages explain how a State applies UN and autonomous sanctions: they are the first stop to learn which authority issues licences and which offences apply. Lists are the designated persons and entities. Announcements show new measures and amendments and are useful for staying current. Legal sources are the laws and regulations. Enforcement entries, 21 in total, include customs press releases, prosecution news and penalty notices; they show how cases are actually detected. The export control entries, also 21, link to control lists, end-user guidance and licensing portals. Licensing and debarment entries total 14: 8 licensing and 6 debarment. The remaining categories include maritime reference, geospatial reference, risk context, an aggregator and a de facto notice. The counts in the table add up to 442 of the 451 entries.

Core sources for export control and enforcement

Authority	Source	Why it helps
US BIS	Denied Persons List; Common High Priority Items	Restricted parties and priority HS codes
US Trade.gov	Consolidated Screening List	One search across several US lists
US State DDTC	Public portal and debarment notices	Defence trade and debarred parties
US DOJ and HSI	Export control enforcement; illicit procurement	Case examples and typologies
US OFAC	General licences; civil penalties	Sanctions authorisations and breaches
EU DG FISMA	Common High Priority Items	Priority items by HS code
UK HMRC and OFSI	Compound settlements; enforcement decisions	Strategic export and sanctions penalties
Japan MOF	Economic sanctions and licensing procedures	Licensing process in Japan

Key point: These are entries marked Core in the registry. Check the official page for the current position.

These are examples of entries that the registry marks as Core priority. There are 143 Core entries in all, 271 Country monitoring entries and 37 Adjacent entries. The Consolidated Screening List allows one search across several US restricted party lists. The BIS Denied Persons List and the Common High Priority Items lists support restricted-party and HS-code screening. The DOJ and HSI pages describe real enforcement cases and typologies and are excellent teaching material. OFAC and OFSI publish general licences and penalty decisions that show how sanctions are enforced.

Using sources safely: a quick routine

- Start from the official publisher, not a mirror or an aggregator
- Check the date and version of the list or notice
- Match names with care: aliases, spellings and identifiers
- Record the source, URL and time of every check in your notes
- Escalate hits and doubtful matches to the competent authority
- Never treat a screening hit alone as proof of an offence

Side box: Remember - A list is a lead, not a verdict; Different States have different lists; Re-check close to the time of action

Teach a simple routine. Begin with the official publisher. Check the date, because lists change often, sometimes daily. Match names with care: transliteration and aliases cause false positives and false negatives, so use identifiers such as registration numbers, addresses, dates of birth, IMO numbers and vessel names to confirm. Record the source, URL and time of each check in your notebook; that record supports your evidence later. Escalate hits and doubtful matches to the competent authority rather than deciding alone. Finally, a hit on a list is a lead: the offence still has to be proven under your national law.

Limits and caveats of the registry

- **Not a legal authority:** It is a finding aid. The legal text and the current list are on the official source.
- **No live feed:** All 451 entries are marked as not implemented or end-to-end tested for automated connection.
- **Reuse terms unchecked:** All entries are marked not comprehensively reviewed; check each publisher's terms before reuse.

Key point: Research registry: confirm against the official source before acting.

Be open about the limits of the tool. The registry records where official information is published; it does not interpret the law, and a page may have moved or changed since the research date. Every entry is marked as not implemented or end-to-end tested for automated data connection, so do not build automated screening on the registry alone. Every entry also records that reuse terms were not comprehensively reviewed, so check the publisher's terms before copying content into a training product or system. Many entries note that a feed was not verified, so manual checks of the official page are needed. Where the registry holds only an institutional entry page for a country, officers should ask their national authority for the correct sanctions page.

Chapter 10: Investigation, evidence and cooperation

This chapter moves from detection to investigation. It covers how diversion networks work, how to follow the money, the investigative toolkit, three fictional case scenarios, evidence and chain of custody, penalties, international cooperation and the role of industry.

In this chapter: Diversion typologies; Following the money; Investigation toolkit; Three fictional case scenarios; Evidence and documentation; Penalties; International cooperation; Working with industry

Diversion typologies

- **Front and shell companies:** Newly formed trading companies placed between the supplier and the end-user.
- **Third-country routing:** Goods pass through hubs and weak-control States to hide the destination.
- **False documents:** Forged end-user certificates, licences and invoices.
- **Relabelling and re-invoicing:** Goods repacked, relabelled or re-documented in free zones.
- **Brokers and forwarders:** Intermediaries who arrange the deal and obscure the real parties.
- **Technology transfer:** Drawings, software and know-how moved electronically or by travellers.

These typologies come from public enforcement and expert-panel reports on proliferation and sanctions evasion. Front and shell companies sit between the supplier and the end-user and are often newly formed, with nominee directors and shared addresses. Third-country routing uses hubs and weak-control States to obscure the destination. False documents include forged end-user certificates and altered licences. Relabelling and re-invoicing take place in free zones and warehouses. Brokers and forwarders can hide who the real parties are. Technology transfers can be done without physical goods.

Following the money

- Payments from third countries or from banks unconnected to the buyer
- Trade-based money laundering: over- or under-invoicing and false descriptions
- Ownership hidden by shell companies, nominee directors and layered structures
- Financial intelligence units can trace flows and flag linked accounts
- Request bank and company records through proper legal channels

Side panel: Payments often reveal the true buyer

Payments are often the best evidence of who is really behind a deal. In diversion cases, the buyer named in the documents may be a shell, while the money comes from a different company or country. Trade-based money laundering uses false pricing and descriptions to move value. Beneficial ownership is hidden through layered structures, so company registers and beneficial ownership registers are useful but incomplete. Your financial intelligence unit can trace flows and may already hold reports on the parties. Banks and company records can be requested through your national legal process, and through mutual legal assistance when the records are abroad. Involve financial investigators early.

Investigation toolkit and open-source research

- **Company registers:** Directors, addresses, formation dates, beneficial owners.
- **Sanctions and denied-party lists:** Check all parties, including addresses and aliases.
- **Shipping and tracking:** Vessel position data, container tracking, port calls.
- **Trade data:** Past import and export records and shipment histories.
- **Websites and social media:** Company claims, products, staff and customers.
- **Seizure and case databases:** Prior detections, linked parties and methods.

Open-source research is cheap, fast and often decisive. Company registers show directors, addresses and formation dates; a company formed last month with a residential address and a large order is a red flag. Sanctions and denied-party lists should be searched for all parties, including aliases and addresses. Vessel and container tracking can verify claimed routes and port calls. Trade data can reveal shipment histories and linked parties. Websites and social media show what a company actually does, who its customers are and whether its claims match the goods. Case databases such as the WCO Customs Enforcement Network show prior detections and methods.

Scenario A (fictional): the machine-tool container

What you find

- Export declaration: "spare machinery parts", general machinery tariff code
- Low declared value; consignee is a trading company formed six months ago
- Packing list shows precision multi-axis machining equipment
- No authorisation reference on the declaration
- Destination is a transit hub, not an industrial area

What would you do?

- Which documents do you request first?
- How do you check the classification?
- Who is the real end-user, and how do you find out?
- Release, detain or refer? On what basis?
- Which partner agencies do you alert?

The facts are fictional. Learning points: the description is vague and the value low, so classification is in doubt; the packing list contradicts the declaration and suggests a controlled machine tool; there is no authorisation reference; the consignee is a newly formed trading company and the destination is a hub, so the end-user is unclear. A good answer asks for the technical data sheet and the commercial contract, contacts the licensing authority to check whether any licence exists and to get a classification opinion, uses open sources to research the consignee, detains the goods if there is a legal basis, and alerts customs at the destination hub.

Scenario B (fictional): the transit truck

What you find

- Transit declaration from State X to State Z, goods described as "electronic components"
- Consignee shown as "to order"; notify party is a logistics firm
- Weight on the transport document is higher than on the invoice
- Truck route passes a long detour through a free zone
- Seal number differs from the number on the declaration

What would you do?

- Do you have power to inspect goods in transit?
- What does the weight difference suggest?
- How do you identify the real consignee?
- Which State should you alert, and how?
- What do you record before releasing or holding the truck?

This scenario tests transit knowledge. Learning points: the consignee to order and a logistics firm as notify party hide the real receiver; the weight mismatch suggests the cargo changed or the documents are wrong; the detour through a free zone and the different seal number indicate possible opening, repacking or swapping. Discuss what happens if the State has no transit control: the best response may be information sharing so another State can act.

Scenario C (fictional): the chemical import

What you find

- Import permit for 50 kg of one chemical from a named consignor
- Container holds 500 kg in drums with a different chemical's label
- Consignor on the bill of lading differs from the permit
- Importer is a new company not registered for chemicals
- No delivery confirmation for two earlier consignments

What would you do?

- Which mismatches matter most?
- How do you handle unknown drums safely?
- Who verifies the permit's authenticity?
- Could the goods be diverted after import?
- What do you tell the exporting State?

This scenario applies Chapter 6. Learning points: the quantity, chemical identity and consignor differ from the permit; the importer is not registered; earlier consignments lack delivery verification. First priority is safety: do not open the drums; call trained responders and photograph labels. Verify the permit with the issuing authority through official channels. Consider whether the goods could be diverted or re-exported after import, and inform the exporting State and the licensing authority. Discuss evidence: labels, drum numbers, photographs, permit copies and records of statements. The learning outcome is that import permits give officers a precise baseline to compare goods and parties against.

Evidence and documentation

- Preserve originals and make certified copies of all documents
- Photograph goods, markings, seals and packaging in place
- Keep a chain of custody for samples and seized goods
- Obtain a written classification opinion from the authority or an expert
- Record statements, timelines, sources and screenshots of open-source material

Side box: Evidence checklist - Documents: originals and copies; Goods: photos, seals, labels; People: statements, contact data; Expert: written classification; Digital: devices and messages

Strategic trade cases are won or lost on documentation. Keep original documents and certified copies. Photograph goods and packaging where found, with seals and labels visible. Maintain a chain of custody for samples and seized goods from the moment of discovery. Obtain a written classification opinion from the licensing authority or another recognised expert, because courts will want to know why the goods were controlled. Record statements, sources and timelines, and capture screenshots of web pages and registers. Secure digital devices and messages according to your law.

Measures and penalties

Measure	Purpose
Detention and seizure of goods	Stop the shipment and secure evidence
Administrative fines	Sanction non-compliance without a full trial
Criminal prosecution and imprisonment	Punish serious or deliberate violations
Confiscation of goods and proceeds	Remove illicit gain
Licence suspension, revocation, debarment	Deny future trade to violators
Publication and listing	Deter and inform other agencies

Key point: Penalties are set by national law: complete this table for your own country.

Most legal systems provide a mix of measures. Detention and seizure are first-line actions that stop a shipment and preserve evidence. Administrative fines allow quicker action for less serious breaches. Criminal prosecution is reserved for serious and deliberate violations. Confiscation removes the proceeds. Licence suspension, revocation or debarment denies future trade to violators. Publication of sanctions deters and informs. The balance differs between countries.

International cooperation

- **Customs mutual assistance:** Bilateral agreements and, in the EU, the Naples II Convention.
- **World Customs Organization:** CEN, CENcomm, ContainerComm and the Strategic Trade Control Enforcement programme.
- **INTERPOL and Europol:** Police cooperation, notices and analysis.
- **Licensing authority networks:** Contact points in partner States for licence verification.
- **UNODC and the 1540 Committee:** Training, technical assistance and capacity building.
- **Mutual legal assistance:** Evidence and records for criminal cases abroad.

No State can tackle diversion networks alone. Customs mutual assistance agreements, including the Naples II Convention in the EU, allow customs services to exchange information and request investigative help. The WCO provides secure communications and databases and has a Strategic Trade Control Enforcement programme with tools and guidance. INTERPOL and Europol support police cooperation. Licensing authorities often have contact points in partner States for verifying licences and end-user certificates. UNODC and the 1540 Committee offer training and technical assistance. For criminal cases, mutual legal assistance provides a formal route to evidence abroad.

Working with industry

- Internal compliance programmes: see EU Commission Recommendation (EU) 2019/1318
- Outreach builds awareness and reporting channels
- Forwarders, carriers and port operators see anomalies first
- Voluntary disclosure may be a mitigating factor under national rules
- Share red-flag guidance and feedback with industry

Side panel: Industry is your first line of detection

Compliant companies are partners. Internal compliance programmes set out how a company classifies goods, screens customers and reports problems; the European Commission's Recommendation (EU) 2019/1318 describes good practice, and many authorities require or reward an ICP when granting global licences. Outreach and awareness sessions help companies, forwarders, carriers and port operators recognise red flags and know whom to call. Logistics providers often see anomalies first, such as unusual requests to change a consignee. Many systems treat voluntary self-disclosure as a mitigating factor, but this is a matter of national law,

so check yours. Giving feedback to industry on what you found closes the loop and encourages more reporting.

Chapter 11: Practical exercises and wrap-up

This chapter consolidates the course through exercises, a pocket checklist, a knowledge check, key takeaways and further reading.

In this chapter: Exercise 1: document check; Exercise 2: classification walk-through; Exercise 3: tabletop at the port; Pocket checklist; Knowledge check; Key takeaways; Resources

Exercise 1: spot the differences (fictional)

Field	Authorisation	Shipment found
Exporter	Northgate Precision Ltd	Northgate Precision Ltd
Consignee	Alder Trading FZE	Alder Trading FZE; notify party Karim Logistics
End-user	Meridian Textile Works	Not stated
Items	2 five-axis milling machines	4 machining centres
Destination	Country X	Country Y, via Country X
Validity	1 March to 31 August 2026	Shipped 14 October 2026

Key point: Task: list every discrepancy and decide what you do next.

The expected findings: the quantity is double the authorised quantity; the item description differs; the end-user is missing on the shipment documents; a new notify party appears; the final destination differs and the route passes through the authorised destination; the shipment date is after the licence expired. Discussion questions: which discrepancy is most serious? What is the legal consequence? Do you detain? Who do you call to verify the licence? What documents do you ask the exporter for? What do you record? All names and countries are fictional.

Exercise 2: classification walk-through

1. **Receive:** You are given an invoice and a data sheet for an unfamiliar item.
2. **Find the entry:** Use the correlation table and control list to find candidate entries.
3. **Compare:** Check the data sheet against the parameters of each entry.
4. **Conclude:** Controlled, not controlled or needs expert advice. Explain why.

Exercise 3: tabletop at the port

1. **Alert:** Targeting unit flags a container: vague goods, new consignee, hub routing.
2. **Inspect:** Documents conflict; drums are unlabelled and the smell is unusual.
3. **Escalate:** Isolate, call responders, contact the licensing authority.
4. **Investigate:** Secure evidence, check parties, alert partner customs.
5. **Decide:** Detain, refer for prosecution, or release with conditions.

Officer's pocket checklist

Documents

- Authorisation valid and genuine
- Parties match across documents
- Description and classification fit
- Quantity within balance
- End-user certificate checks out

Goods

- Goods match the paperwork
- Markings, serial numbers photographed
- Unknown items: isolate, do not open
- Expert advice requested if unsure
- Seals and containers recorded

Action and record

- Release, detain or refer
- Alert partners and licensing authority
- Chain of custody kept
- Notes and photos saved
- Report filed

This one-page checklist can be printed on a card. Documents: confirm that the authorisation is valid and genuine, that the parties match across all documents, that the description and classification fit the goods, that the quantity is within the balance, and that the end-user certificate is credible. Goods: confirm that they match the paperwork, photograph markings and serial numbers, isolate and do not open unknown items, request expert advice when unsure, and record seals and container numbers. Action and record: decide to release, detain or refer; alert partners and the licensing authority; maintain the chain of custody; save notes and photographs; file the report.

Knowledge check

- Which UN resolution requires controls on transshipment of WMD-related items?
- What does a catch-all clause do?
- Why is the tariff code not enough to classify an item?
- Name two documents you compare in a transit check
- What is delivery verification?
- What is your first step with unlabelled drums?

Side panel: Answer orally or in teams. Answers are in the speaker notes

Use this as a quick oral quiz or a team game. The answers: Resolution 1540 of 2004. A catch-all clause lets the authority require a licence for items that are not on the control list when the end-use is of concern. The tariff code describes what a good is, while the control list describes technical performance, so one code can include controlled and non-controlled items. In transit, compare for example the bill of lading, the manifest, the transit declaration and the invoice. Delivery verification is the importer's confirmation of receipt, sent back to the exporting State. With unlabelled drums: isolate the area, do not open or test, photograph, and call trained responders.

Key takeaways

- **Classify first:** The tariff code is not enough. Compare technical data with the control list.
- **Documents must agree:** Licence, invoice, transport papers and goods must tell the same story.
- **Hubs are targets:** Transit and transshipment need risk profiling and information sharing.
- **Import is half the chain:** Import permits and delivery checks complete the picture.
- **Safety and evidence:** Isolate unknown goods, document everything, keep chain of custody.
- **Know who to call:** Licensing authority, experts, partner customs and prosecutors.

Close with six messages. Classify first: tariff codes are not enough, and technical data is needed. Documents must agree: if the licence, invoice, transport documents and goods tell different stories, stop and verify. Hubs are targets: transit and transshipment need risk profiling and information sharing. Import is half the chain: import permits and delivery verification complete the picture. Safety and evidence: isolate unknown goods and document everything. Know who to call: the best officers know their contacts before the shipment arrives.

Resources and further reading

Topic	Where to look
EU Dual-Use Regulation and Annex I	eur-lex.europa.eu ; policy.trade.ec.europa.eu
Wassenaar Arrangement control lists	wassenaar.org
Nuclear Suppliers Group	nuclearsuppliersgroup.org
Missile Technology Control Regime	mtcr.info
Australia Group	australiagroup.net
UN Security Council Committee 1540	un.org/en/sc/1540
WCO Strategic Trade Control Enforcement	wcoomd.org
Container Control Programme and UNODC	unodc.org
Chemical Weapons Convention and OPCW	opcw.org
Official sanctions and export-control pages	Global Sanctions Source Registry (Module 9), then the official publisher

These are the official websites where the current control lists, legal texts and guidance can be found. For the EU, use EUR-Lex for the consolidated text of Regulation (EU) 2021/821 and the European Commission's trade policy site for guidance, general authorisations and the latest Annex I update. For the regimes, use the regime websites. For customs enforcement tools and guidance, the WCO. For capacity building and the Container Control Programme, UNODC.

Annex A: Document checklists

Export authorisation

- Issued by the competent authority; reference number verifiable
- Exporter, consignee and end-user match the shipping documents
- Items, quantities and control-list entry match the goods
- Valid on the date of shipment; quantity not exhausted
- Destination and route within the authorisation; conditions met
- No sign of alteration; copy not substituted for the original where an original is required

End-user statement or certificate

- Signed by a named, authorised person with title
- Company exists at the stated address; business fits the goods
- States end-use and, where used, a no re-export commitment
- Dates consistent with the order; no generic or recycled wording
- Authenticity confirmed with the issuing authority where in doubt

Transit or transshipment documents

- Transit declaration, bill of lading or airway bill consistent with each other
- Origin, destination and routing make commercial sense
- Authorisation for transit, where the transit State requires one
- Seals intact; container or packaging unchanged since loading
- Notify party and consignee match the trade

Import permit or certificate

- Issued by the importing State's competent authority
- Importer registered; quantity and substance or item match
- Consignor and consignee match the shipping documents
- Valid dates; certificate and delivery verification procedure followed
- Prior consignments consistent with the importer's profile

Annex B: Red-flag matrix

Area	Examples	First action
Customer	New customer; no web presence; business unrelated to goods; refuses end-use information	Verify identity and business; ask the exporter for background
Deal	Cash or third-party payment; unusually favourable price; urgency; refusal of installation or training	Check payment chain and commercial logic
Route	Unusual routing; destination changed after departure; several hubs with no reason; repacking in a free zone	Request routing explanation; alert transit and destination partners
Documents	Vague description; quantity or party mismatch; altered dates; copy only	Verify with the issuing authority; compare with goods
Goods	Markings removed; goods differ from description; over-specified for stated use	Photograph, isolate, get technical expert advice

Red flags are indicators for further enquiry. No single indicator proves an offence; several together justify detention for verification under your national powers.

Annex C: Glossary

Term	Meaning
Dual-use item	Goods, software or technology with both civil and military or WMD-related uses.
Strategic goods	Items whose export, transit or transfer a State controls for security reasons, including dual-use and military items.
Control list	The legal list of controlled items, for example Annex I of Regulation (EU) 2021/821, based on the multilateral regimes.
Catch-all clause	A rule requiring authorisation for non-listed items when the exporter knows or is told of a concerning end-use.
End-user certificate (EUC)	A document from the recipient stating who will use the goods and for what, often with a no re-export promise.
International Import Certificate (IIC)	A document from the importing State's authority confirming it knows of and accepts the import.
Delivery Verification Certificate (DVC)	Proof that the goods arrived, issued by the importing authority.
Transit	Goods passing through a State on the way to another State, without being released for local use.
Transshipment	Moving goods from one vessel or aircraft to another at an intermediate point.
Brokering	Arranging a transfer of controlled items between third countries; often needs a licence.
Technical assistance	Services such as repair, training or know-how that can support controlled items.
Intangible technology transfer	Transfer of software or technology by email, cloud or oral explanation.
Wassenaar Arrangement	Regime for conventional arms and dual-use goods, founded 1996.
Nuclear Suppliers Group	Regime for nuclear and nuclear-related dual-use items, founded 1975.
Missile Technology Control Regime	Regime limiting missile and UAV technology, founded 1987.
Australia Group	Regime for chemical and biological precursors and equipment, founded 1985.
Zangger Committee	Group that interprets nuclear export controls under the NPT, founded 1971.
UNSCR 1540	UN Security Council resolution (2004) requiring States to control WMD-related items, including transit and transshipment.
Common High Priority Items	Dual-use items identified by HS code as found in weapons used on the battlefield; targeted by sanctions authorities.
Chain of custody	Documented record of who held evidence and when, from seizure to court.
5x5x5	Intelligence grading of source reliability, information accuracy and handling code.
OSINT / FININT	Open-source intelligence and financial intelligence.

Annex D: Official sources

Topic	Where to look
EU Dual-Use Regulation and Annex I	eur-lex.europa.eu ; policy.trade.ec.europa.eu
Wassenaar Arrangement control lists	wassenaar.org
Nuclear Suppliers Group	nuclearsuppliersgroup.org
Missile Technology Control Regime	mtcr.info
Australia Group	australiagroup.net
UN Security Council Committee 1540	un.org/en/sc/1540
WCO strategic trade control enforcement	wcoomd.org
Container Control Programme and UNODC	unodc.org
Chemical Weapons Convention and OPCW	opcw.org
Official sanctions and export-control pages	Global Sanctions Source Registry (451 entries; finding aid only), then the official publisher

Always use the official publisher and check the date of any list or notice before acting on it.