Operational Manual

Sanctions Compliance and the Prevention of Illicit Transactions related to the procurement of Advanced Conventional Weapons Components and other Sensitive Technologies

2026

Operational Manual

Sanctions Compliance and the Prevention of Illicit Transactions related to the procurement of Advanced Conventional Weapons Components and other Sensitive Technologies

Authors: Tatiana Ursu

Contributors: Giorgi Goguadze, Nikoloz Kipshidze

Table of Contents

Introduction

This Operational Manual provides a practical framework for the implementation of sanctions compliance, restrictive measures and export, re-export, import and transit control obligations related to sensitive goods, technologies and software with dual-use or military applications. It is designed as a hands-on tool to support the identification, assessment and mitigation of risks in accordance with the legal framework of the Republic of Moldova which applies international and European Union standards.

The Manual supports the consistent application of risk-based controls in day-to-day operations. It reflects the need for competent authorities and economic operators to apply controls in a structured and practical manner across supply chains, taking into account evolving trade patterns and emerging risks.

It provides an operational overview of international sanctions regimes and export control systems, with a focus on identifying and managing risks related to illicit procurement networks, diversion practices and the misuse of Advanced Conventional Weapons (ACW) components and other sensitive technologies subject to trade restrictions.

Effective sanctions and export control measures are essential to prevent the diversion of sensitive goods and technologies to unauthorized end-users or prohibited destinations. Their proper implementation contributes to reducing proliferation risks, strengthening enforcement practices and ensuring the integrity of international trade flows.

The Republic of Moldova remains committed to strengthening its alignment with international sanctions regimes and European Union restrictive measures, while continuously enhancing its national enforcement and compliance capacities in response to evolving trade and security risks. This commitment is grounded in the constitutional obligation of Moldova to respect international law and to fulfil in good faith its international obligations, as stipulated in Art.8 of the Constitution of the Republic of Moldova.

General Framework of Advanced Conventional Weapons (ACW)

Definition and Scope

Advanced conventional weapons (ACWs) encompass a broad spectrum of highly sophisticated military systems. Although there is no universally agreed definition, the term generally refers to systems such as man-portable air defence systems (MANPADS), anti-tank guided missiles (ATGMs) and large-scale military platforms including tanks, aircraft and missile systems. It also includes enabling technologies such as sensors, laser systems and precision-guided munitions. Ballistic and cruise missiles are also increasingly used in conventional military operations and are therefore considered part of the broader ACW framework.

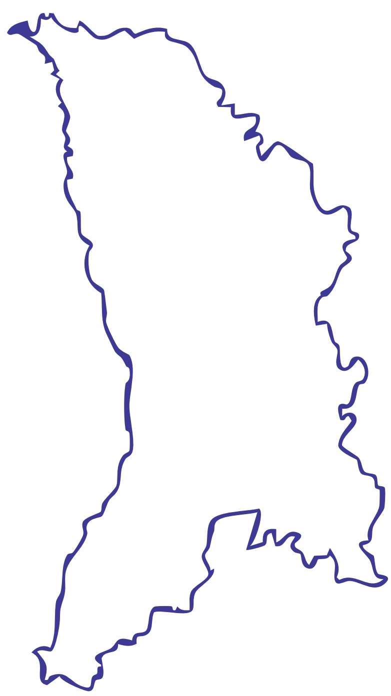
For compliance purposes, a key challenge lies not only in complete systems, but also in the identification and control of individual components within the ACW-related supply chain. Many of these items qualify as dual-use goods and require enhanced due diligence and end-use verification.

The ACW-related supply chain relies on a wide range of industrial and technological components, many of which originate in civilian production but may be integrated into military systems.

Procurement and Proliferation Networks within the ACW-Related Supply Chain

The networks operating within the ACW-related supply chain generally consist of three main categories of actors: *intentional proliferators, complicit intermediaries and unintentional participants.*

All three categories may be relevant in the context of the Republic of Moldova, particularly due to its geographic position along regional trade and transit routes, which may expose economic operators to indirect proliferation risks and requires heightened vigilance from companies operating in this environment.



Intentional proliferators are state or non-state actors directly engaged in the acquisition, development, or transfer of materials and technologies within the ACW-related supply chain.

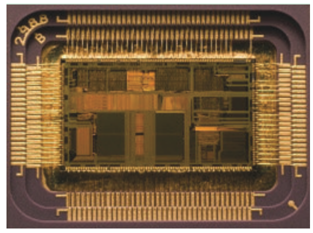
Complicit intermediaries knowingly facilitate such activities by providing logistical, financial, or technical support even and theoretical support, often with the aim of circumventing sanctions and export control measures.

Unintentional participants, such as manufacturers, freight forwarders, financial institutions and other service providers, may become involved without awareness of the final end-use, typically due to deceptive documentation or insufficient compliance controls.

High-Risk Goods within the ACW-Related Supply Chain

Due to their relatively small size and the resulting difficulty in detection and traceability, ACW components represent a significant concern in the context of proliferation, often more so than complete systems.

To mitigate these risks, both private sector entities and public authorities should place strong emphasis on due diligence procedures, thorough licensing assessments and effective end-use verification. Particular attention should be given to key categories of components commonly identified within the ACW-related supply chain, as illustrated in the table below.

Type of Component	Usage / Application	Examples / Notes	Illustration / Icon
Microelectronics / Microchips	Basic electronic components in conventional weapon systems	Processors, memory chips, control circuits	
Semiconductors	Communications equipment, unmanned aerial systems (UASs), precision long-range munitions	Power transistors, diodes, integrated circuits	
Bearings	Engines, vehicle parts	Ball bearings, used in tanks, helicopters, and military engines, submarines	
Connectors, Fasteners, Transformers, Casings, Transistors, Insulators	Defence-related components (computers, sensors, switches, amplifiers)	Basic components that constitute electronics systems in a conventional weapon system	
Engines, Vehicle Parts	Tanks, aircraft, submarines, other military systems	Tanks, armoured combat vehicles (ACVs), aircraft (turbines)	
Composite Material	Tanks, armoured combat vehicles (ACVs), aircraft	Carbon fiber panels, resistant lightweight structural parts, Aircraft wings	

The categories presented above reflect typical dual-use components that, while widely used in civilian industries, may be integrated into military systems. Their identification and control are essential for effective risk management and compliance.

These components are particularly vulnerable to diversion, including through misleading or fraudulent declarations regarding their end-use or end-user. As such, focusing compliance and enforcement efforts on these items is critical for preventing unauthorized military applications, including system upgrades and reverse-engineering activities.

In contrast, shipments involving large-scale or legacy military systems, such as tanks or artillery, are generally easier to detect and intercept due to their size, logistical requirements and visibility within international transport systems. However, such platforms often require continuous modernization, creating sustained demand for spare parts, advanced subsystems and technical expertise—further increasing the relevance of controlling individual components within the supply chain.

Patterns of Proliferation in the ACW-Related Supply Chain

In general, the proliferation of ACW-related goods, components and technologies follows several recurring pathways, often involving complex and multi-layered supply chains.

The most common proliferation patterns are illustrated below:

Direct peer-to-peer transfers:

State-level or direct exchanges of weapons, components or technologies, including re-circulation among partners

Covert transshipment:

Movement of dual-use goods through intermediaries using falsified or incomplete documentation to conceal end-user or destination.

Domestic replication:

Use of imported components or technologies in domestic production, including reverse engineering and system upgrades.

Uncontrolled diffusion:

Further transfer of components or technologies to third parties, reducing traceability and increasing proliferation risks.

These patterns reflect typical methods through which controlled or sensitive goods may be transferred, concealed or repurposed within international trade flows.

In practice, such patterns are often supported by a range of operational mechanisms, including:

- indirect procurement through intermediaries, where controlled goods are acquired via third parties to conceal the identity of the final end-user;
- transshipment and re-export schemes, involving the routing of goods through multiple jurisdictions to obscure their origin and destination;
- misrepresentation of end-use or end-user, including the use of falsified or incomplete documentation to justify otherwise restricted transactions;
- use of front companies or shell entities, established to facilitate procurement activities while masking the involvement of sanctioned or high-risk actors;
- diversion of dual-use goods, where items intended for legitimate civilian purposes are subsequently redirected toward unauthorized military applications;
- procurement of components for system upgrades or reverse engineering, particularly in cases where access to complete systems is restricted.

These mechanisms are frequently used in combination and may evolve over time, increasing the complexity of detection and enforcement.

The patterns and mechanisms described in this section are based on commonly identified proliferation typologies reflected in international practice, including frameworks and guidance developed by the United Nations Security Council, the Financial Action Task Force, the Wassenaar Arrangement and the European Union dual-use export control regime.

In the context of the Republic of Moldova, the risk environment is shaped by its strategic location along regional trade and transit corridors, which may expose economic operators to indirect proliferation dynamics. These include covert transshipment practices, misrepresentation of end-users and the potential re-routing of sensitive dual-use goods within complex and multi-layered supply chains.

Proliferation and Diversion Risks

The proliferation of ACW-related components and technologies poses substantial risks to national and international peace and security. These risks are further amplified by the increasing accessibility of advanced technologies, the globalization of supply chains and the use of complex trade routes involving multiple intermediaries.

Diversion may occur when goods intended for legitimate civilian use are redirected towards unauthorized military applications or end-users. Such risks are particularly pronounced in cases involving insufficient transparency regarding the end-user or end-use, as well as in jurisdictions subject to international sanctions or embargo measures.

In addition, certain country-specific structural factors may further influence the risk environment. In particular, the presence of administrative-territorial units located on the left bank of the Nistru River, which are not under the effective control of the constitutional authorities, may present additional challenges related to the transparency and traceability of economic activities.[1]

[1] https://statistica.gov.md/ro/comert-exterior-60.html

From a compliance perspective, this context may increase exposure to risks associated with transshipment and re-export operations, including the potential redirection of goods toward higher-risk destinations, as well as the use of intermediary entities and complex trade arrangements.

At the same time, limitations in the availability and consistency of statistical data related to economic activities in this region may affect the ability of both authorities and private sector operators to conduct effective risk assessments and due diligence procedures.[2]

Specific Risk Factors Related to the Left Bank of the Nistru River

The presence of administrative-territorial units located on the left bank of the Nistru River represents a specific structural risk factor within the Republic of Moldova's compliance environment. Due to the limited effective control exercised by constitutional authorities in this area, economic activities may lack full transparency and regulatory oversight.

From a compliance perspective, this situation may create vulnerabilities related to:

- reduced traceability of goods and transactions;
- increased exposure to informal or unregistered economic activities;
- potential use of intermediary entities or storage locations for transshipment purposes;
- challenges in verifying end-users and end-use of goods originating from or routed through the region.

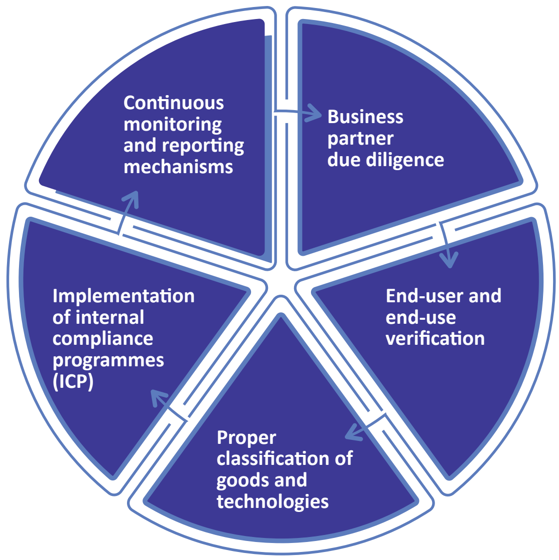
These factors may increase the risk of diversion of dual-use goods and other sensitive technologies, particularly in the context of complex supply chains and indirect trade routes. Economic operators should therefore apply enhanced due diligence measures when transactions involve counterparties, logistics routes or goods that may be connected to this region.

At the same time, limitations in the availability and reliability of statistical data related to trade flows associated with this area may affect risk assessment processes and require a more cautious, risk-based approach from both authorities and private sector actors.

[2] https://expert-grup.org/ro/biblioteca/mega-analiza-cresterii-economice-in-moldova/itemlist/category/186

Importance for Compliance Systems

Effective control of risks within the ACW-related supply chain requires the implementation of robust compliance systems by economic operators, supported by coordinated actions of competent authorities. In the context of increasing complexity of supply chains and evolving proliferation risks, a risk-based approach is essential to ensure that controls are applied in a consistent and proportionate manner. The key elements of an effective compliance system are illustrated here →



In practice, these elements include:

01. proper classification of goods and technologies, ensuring that items subject to export control or sanctions regimes are correctly identified;

02. end-user and end-use verification, aimed at confirming the legitimacy of the final destination and intended use of goods;

03. business partner due diligence, including the assessment of customers, intermediaries and other actors involved in the transaction;

04. implementation of internal compliance programmes (ICP), establishing internal procedures, controls and responsibilities for managing compliance risks;

05. continuous monitoring and reporting mechanisms, allowing for the identification of suspicious transactions and timely communication with competent authorities.

These elements should not be applied in isolation, but as part of an integrated compliance framework that reflects the specific risk profile of the operator and the nature of its activities.

The consistent application of these measures is essential for preventing diversion, ensuring compliance with sanctions and export control obligations and maintaining a secure and transparent trade environment.

International Sanctions Regimes and Export Control Frameworks

The international security and trade environment is shaped by the combined application of sanctions regimes and export control frameworks. These instruments function as complementary mechanisms aimed at restricting access to sensitive goods, technologies and financial resources, and preventing their misuse.

Sanctions primarily target specific states, entities and individuals through restrictions on financial transactions, trade and services. In parallel, export control systems regulate the transfer of strategic goods and technologies through licensing requirements, risk assessments and end-use/end-user verification.

For economic operators, these frameworks create overlapping legal obligations, particularly in sectors involving dual-use goods, logistics, manufacturing and financial services. Compliance therefore requires an integrated approach combining sanctions screening with export control procedures.

In the Republic of Moldova, alignment with international and European Union standards has increased regulatory expectations, requiring both public authorities and private sector entities to implement structured compliance and due diligence mechanisms.

International Sanctions Regimes and Restrictive Measures

International sanctions regimes are a key instrument of global security governance, adopted in response to threats to international peace and security or violations of international law.

For the Republic of Moldova, the practical implementation of restrictive measures is primarily linked to the progressive alignment with the European Union Common Foreign and Security Policy (CFSP), including restrictive measures targeting dual-use goods, sensitive technologies, military-related items and procurement networks associated with sanctioned jurisdictions.

While United Nations Security Council sanctions remain binding under international law and represent an essential component of the international security framework, the European Union sanctions framework has particular practical relevance for Moldova’s compliance environment.

In recent years, EU restrictive measures have increasingly focused on preventing sanctions circumvention, intermediary procurement schemes and unauthorized transfers of dual-use goods and sensitive technologies.

International Export Control Regimes

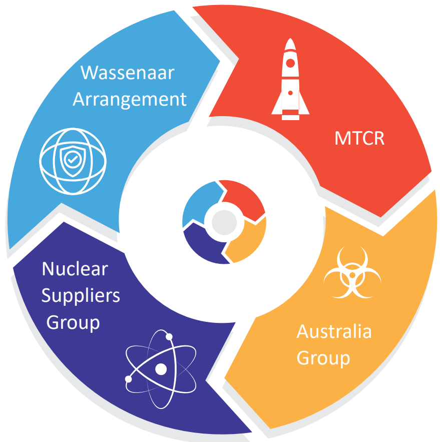
International export control regimes form a central component of the global non-proliferation framework. Unlike sanctions, which are primarily restrictive, export controls are preventive in nature and regulate the transfer of sensitive goods, dual-use technologies, software and technical assistance.

These systems operate through:

- control lists;
- licensing requirements;
- end-use and end-user risk assessments.

At the international level, export control efforts are coordinated through four main multilateral regimes:

- the Wassenaar Arrangement – covering conventional arms and dual-use goods;
- the Missile Technology Control Regime – addressing delivery systems for weapons of mass destruction;
- the Nuclear Suppliers Group – governing nuclear-related exports;
- the Australia Group – focusing on chemical and biological materials.



Within the European Union, export controls are harmonized through Regulation (EU) 2021/821, which governs export, transit, brokering and technical assistance related to controlled items.

For the Republic of Moldova, alignment with international and EU standards has strengthened the national control system. Economic operators are required to:

- obtain authorization for controlled exports and transit;
- conduct end-use and end-user due diligence;
- implement internal compliance programmes.

Particular attention is required for dual-use goods due to their potential civilian and military applications.

It should be noted that the Republic of Moldova is not a participating state in the Wassenaar Arrangement. However, its national system demonstrates a high degree of alignment with the principles and control lists of this regime.[3]

Despite the existence of a comprehensive legal framework, practical implementation challenges remain, particularly within the private sector, due to limited technical capacity, varying levels of awareness and resource constraints.

Accordingly, economic operators must ensure that decisions related to procurement, logistics and business partnerships reflect increased regulatory scrutiny and evolving risk conditions.

[3] https://www.wassenaar.org/participating-states/

Best Practices for Compliance with Sanctions and Export Control Regimes

In addition to the general compliance elements outlined above, economic operators should apply practical measures designed to prevent involvement in illicit procurement networks, sanctions evasion schemes and unauthorized transfers of controlled or sensitive goods.

A basic sanctions and export control compliance framework should include the following components:

Risk assessment. Economic operators should identify and assess their exposure to sanctions and export control risks, taking into account the nature of goods handled, business partners, geographic exposure, supply chains, transit routes and potential links to high-risk jurisdictions or sanctioned end-users.

List-based screening. Operators should conduct systematic screening of customers, suppliers, intermediaries, beneficial owners and other relevant parties against applicable sanctions and restricted party lists, including United Nations, European Union and national restrictive measures lists.

Targeted screening. In addition to list-based screening, operators should apply enhanced checks where transactions involve sensitive goods, unusual destinations, intermediary jurisdictions, sectors associated with military or dual-use applications, or companies operating in high-risk environments.

Internal policies and procedures. Companies should establish written internal procedures defining responsibilities, decision-making processes, escalation mechanisms and steps to be taken when potential sanctions or export control risks are identified.

Training and awareness. Regular training should be provided to employees involved in procurement, sales, logistics, customs clearance, finance and compliance functions, in order to ensure that staff can identify risk indicators and understand applicable legal obligations.

Record-keeping and audit. Operators should maintain adequate records of due diligence checks, end-user documentation, licensing decisions, correspondence and transaction reviews. Periodic internal audits should be conducted to verify the effectiveness of compliance procedures.

National Framework for the Control of Trade in ACW and Strategic Goods

Republic of Moldova's Commitments to International Sanctions and Alignment with Restrictive Measures

The Republic of Moldova has progressively strengthened its commitment to the implementation of international restrictive measures, developing a national compliance framework grounded in obligations arising from the United Nations system, alignment with the European Union's sanctions regimes and the establishment of domestic enforcement mechanisms.

At the international level, Moldova adheres to restrictive measures adopted by the United Nations Security Councils and demonstrates a high degree of alignment with the restrictive measures adopted by the European Union under its Common Foreign and Security Policy (CFSP).

At the national level, implementation is governed by Law No. 25/2016 on the application of international restrictive measures. This framework defines the scope of sanctions, establishes procedures for their transposition into domestic legal acts and assigns responsibilities to competent authorities. It provides key enforcement tools, including the freezing of funds, restrictions on financial transactions and prohibitions on the provision of economic or technical assistance to designated persons or entities.

Institutional implementation is ensured through a coordinated inter-agency framework involving foreign policy, financial supervision, customs and law enforcement authorities. A central coordinating role is exercised by the Interinstitutional Supervisory Council, which facilitates information exchange, monitors compliance risks and supports consistent implementation.

Operationally, sanctions implementation is supported by the national consolidated list of designated persons and entities, which integrates international designations and serves as a key tool for screening and due diligence.

While Moldova has established a comprehensive legal and institutional framework aligned with international and European standards, practical implementation challenges may persist, particularly within the private sector, due to capacity constraints, varying levels of awareness and resource limitations.

Moldova's sanctions framework has also evolved in the context of its engagement with regional cooperation structures. In recent years, the Republic of Moldova has taken steps toward withdrawal from certain frameworks associated with the Commonwealth of Independent States (CIS), with the objective of ensuring full consistency with its international sanctions' obligations and alignment with European regulatory standards.[4]

In parallel, sanctions implementation is increasingly interconnected with trade control and non-proliferation considerations, particularly in relation to dual-use goods and sensitive technologies. This functional overlap reinforces Moldova's broader compliance architecture.[5]

Recent enforcement cases further illustrate the practical relevance of these risks in the Moldovan context *(see Annex II).*

[4] https://gov.md/en/press-releases/government-initiates-moldovas-withdrawal-statutory-bodies-cis?utm_source=chatgpt.com

[4] https://www.eeas.europa.eu/moldova/european-union-and-republic-moldova_en?s=223

[5] https://legal.un.org/repertory/art41.shtml

[5] https://fpi.ec.europa.eu/what-we-do/common-foreign-and-security-policy_en

Three-Level Sanctions Implementation Framework (UN–EU–National):

International Level

- sanctions adopted by the United Nations Security Council
- binding on member states
- legal basis: Chapter VII of the UN Charter

Regional Level

- sanctions adopted by the European Union
- part of the CFSP (Common Foreign and Security Policy)
- sometimes more extensive than those of the UN

National Level

- transposition of UN and EU sanctions into domestic legislation
- implementation through:
- national law (e.g. Law 25/2016)
- authorities (customs, banks, police, etc.)
- effective enforcement mechanisms

National Strategic Trade Control Legislation, Institutional Structure and Roles of Authorities Responsible for Strategic Trade Control

Pursuant to Law No. 213/2024 on the control of trade in strategic goods, a permanent inter-institutional Commission has been established to coordinate, implement and supervise the national strategic trade control system.

The Commission performs regulatory, advisory and supervisory functions, including:

- oversight of international obligations related to non-proliferation;
- coordination between national authorities;
- review and approval of licensing decisions;
- assessment of transactions involving non-listed goods under catch-all provisions.

Through these functions, the Commission ensures coherence between national legislation, international commitments and operational enforcement.

Licensing Procedures for Strategic Goods

A core operational element of the national control system is the licensing process governing activities involving strategic goods.

The procedural framework is established under Government Decision No. 24/2025, which sets out detailed rules for applications related to export, re-export, transit, brokering and technical assistance.

From an operational perspective, the licensing process follows a sequence of key steps:

- Submission of application: the economic operator submits a complete application file, including technical specifications, end-user and end-use information, and supporting documentation;
- Verification and examination: the competent authority verifies the completeness of the application and circulates it for inter-agency consultation and risk assessment;
- Evaluation: the application is assessed against control lists, catch-all provisions and relevant risk indicators, including end-user and end-use considerations;
- Decision-making: the inter-institutional Commission adopts a decision (approval, refusal or conditional authorization);
- Issuance of authorization: the authorization is formally issued following the decision;
- Post-licensing monitoring: compliance with authorization conditions is subject to verification by competent authorities.

Particular attention is required for dual-use goods due to their potential civilian and military applications and the increased risk of diversion toward unauthorized end-users or prohibited destinations.

The licensing process is increasingly supported by electronic systems, enhancing transparency, traceability and coordination between institutions. The regulatory framework is closely aligned with Regulation (EU) 2021/821, including the application of risk-based assessment procedures and control mechanisms. The licensing process is implemented through a coordinated inter-institutional mechanism, involving several authorities with distinct roles, as outlined below:

Institution	*Role in Commission*	*Key Responsibilities*
Ministry of Economic Development and Digitalization	Chair	Coordinates national policy, aligns with international sanctions and export control regimes, supervises implementation of dual-use goods regulations
Ministry of Defence	Vice-Chair	Provides military expertise, identifies dual-use items with potential military applications
Public Services Agency	Secretary	Administrative coordination, documentation, licensing processes, maintaining registers of controlled goods
Ministry of Foreign Affairs	Member	Supports international cooperation, ensures international obligations are integrated into national procedures
Office for Prevention and Fight against Money Laundering	Member	Monitors compliance, identifies potential violations, coordinates enforcement actions
Information and Security Service	Member	Provides risk assessment and intelligence on end-users, trade flows, and potential diversion of sensitive goods
Ministry of Internal Affairs	Member	Supports enforcement, investigation, and operational oversight for export control breaches
Customs Service	Member	Controls physical movement of dual-use goods at borders, ensures exports/imports comply with licensing and regulations

This institutional structure ensures that licensing decisions are based on a comprehensive assessment of security, regulatory and enforcement considerations.

It should be noted that the Republic of Moldova is not a participating state in the Wassenaar Arrangement, although its national system demonstrates a high degree of alignment with its principles.

Risk Assessment and Inter-Agency Coordination in Strategic Trade Control

Beyond the formal licensing framework, effective strategic trade control requires the operational use of risk assessment tools and coordinated inter-agency mechanisms. The effective prevention of proliferation and illicit trade of ACW and related components requires the practical application of both analytical and coordination tools. In the Republic of Moldova, recent developments have strengthened this approach through the use of the National Risk Assessment (NRA)[6] and the establishment of the National Crisis Management Centre (NCMC)[7].

The NRA represents a national strategic assessment mechanism designed to identify, evaluate and understand risks related to money laundering, terrorist financing and proliferation financing. The NRA supports the implementation of a risk-based approach by competent authorities and private sector entities and contributes to the prioritization of national control and enforcement measures.

The NCMC represents an interinstitutional coordination mechanism established to ensure rapid information exchange and coordinated response in situations involving significant national security, crisis or strategic trade control risks.

01. Practical use of the NRA

The NRA serves as an operational reference tool for identifying and prioritizing risks relevant to proliferation and illicit trade. In practice, authorities and economic operators should use NRA findings to:

- identify high-risk goods categories, trade routes and jurisdictions;
- detect risk indicators such as unusual transaction patterns, use of intermediaries or inconsistencies in documentation;
- support risk-based controls, including customs targeting and selection for inspection;
- enhance due diligence on end-users and end-use, particularly in transactions involving sensitive goods;
- align internal compliance procedures with identified national risk priorities.

The NRA is particularly useful in detecting typologies such as trade-based money laundering and the misuse of corporate structures, which may be used to conceal the diversion of controlled goods.

02. ***Practical use of the NCMC for coordinated response***

In situations where risks exceed the capacity of a single authority or involve complex, cross-sectoral elements, coordinated action is required. In this context, the Government Decision No. 579/2025 on the organization and functioning of the NCMC establishes the legal framework for the functioning of the NCMC.

[6] https://spcsb.md/wp-content/uploads/2025/12/NRA_rezumat.pdf
[7] https://www.cnmc.gov.md/ro/organigrama

The NCMC may be engaged in cases such as:

- detection of complex illicit procurement networks involving multiple jurisdictions;
- suspected large-scale sanctions evasion schemes;
- incidents involving diversion or attempted export of strategic or sensitive goods;
- situations requiring rapid information exchange between customs, financial intelligence, law enforcement and regulatory authorities.

Through this mechanism, authorities can:

- ensure rapid information-sharing between institutions;
- coordinate joint actions and investigations;
- align risk assessments and operational responses;
- manage high-impact cases in a structured and centralized manner.

03. *Operational integration of tools*

The combined use of the NRA and NCMC strengthens the national capacity to prevent and respond to proliferation risks. In practice:

- the NRA supports early identification of risks and vulnerabilities;
- the NCMC enables coordinated response in complex or high-risk situations.

This integrated approach enhances operational effectiveness, improves interagency cooperation and supports the consistent implementation of control measures in line with international standards.

Awareness and Compliance of Economic Operators Handling Strategic Goods

Economic operators engaged in the trade of strategic goods play a central role within the national export control system, as they constitute the primary interface between regulatory requirements and practical commercial activities. Their compliance obligations are designed to ensure that the transfer, transit, brokering and export of strategic goods are conducted in accordance with Law No. 213/2024 and applicable international non-proliferation commitments.

At the core of the compliance framework lies the principle of preventive control, whereby economic operators are required to implement internal mechanisms that ensure early identification and mitigation of proliferation-related risks. These obligations include *proper classification of goods, verification of end-users, maintenance of transaction records, and prior authorization for activities involving controlled items.*

A key instrument in ensuring effective compliance is the implementation of Internal Compliance Programs (ICP). ICP represent structured internal frameworks adopted by economic operators to ensure systematic adherence to export control regulations and to mitigate the risk of unauthorized diversion of strategic goods.

ICP typically include end-user screening, transaction risk assessment, internal authorization procedures, record-keeping systems, employee training, and mechanisms for reporting suspicious activities. These components ensure that compliance is embedded within the operational structure of the company rather than treated as a reactive obligation. The implementation of ICP contributes significantly to strengthening national export control effectiveness by enabling a risk-based approach to compliance. Operators with robust internal control systems facilitate the work of competent authorities by ensuring greater transparency and traceability of transactions involving strategic goods. This approach is consistent with international best practices promoted within the European Union export control framework and multilateral regimes such as the Wassenaar Arrangement.

Public authorities play an important role in promoting awareness and supporting compliance among economic operators through guidance materials, consultations and administrative oversight. This contributes to the development of a compliance-oriented culture within the private sector.

In the context of the Republic of Moldova, several economic sectors may present elevated exposure to proliferation and sanctions evasion risks. These include trade in electronics and microelectronics, machinery and automotive components, logistics and freight forwarding services, as well as financial institutions facilitating cross-border transactions.

Operators in these sectors should apply enhanced scrutiny to transactions involving high-risk goods, counterparties located in jurisdictions with weak regulatory oversight, or complex supply chain structures involving multiple intermediaries.

From a practical perspective, compliance should be embedded into daily business operations. This includes integrating screening mechanisms into procurement processes, verifying beneficial ownership structures, monitoring transaction patterns and establishing internal escalation procedures for suspicious activities.

Sectors Exposed to Elevated Sanctions and Proliferation Risks

In the context of ACW-related procurement and sanctions evasion risks, particular attention should be given to economic sectors that may be more exposed to illicit procurement attempts. These include:

Financial institutions, which may facilitate payments, trade finance, letters of credit, insurance, correspondent banking transactions or other financial services linked to cross-border trade operations.

Electronics and microelectronics companies, including importers, exporters, distributors and resellers of electronic components, semiconductors, integrated circuits, sensors or other items that may have dual-use or military applications.

Logistics and transportation operators, including freight forwarders, customs brokers, air cargo operators, road transport companies and warehouse service providers, which may be used to facilitate transshipment, re-export or concealment of the true destination of goods.

Defence-related companies and manufacturers, including entities involved in the production, repair, modernization or supply of military or dual-use equipment, components or technical services.

IT companies, universities and research institutions, particularly where activities involve software, algorithms, source code, technical data, engineering research or other intangible transfers that may have dual-use applications.

Operators active in these sectors should apply enhanced due diligence measures and ensure that sanctions screening, end-user verification and transaction monitoring are integrated into their internal compliance procedures.

These sectors may be intentionally targeted by procurement networks seeking to exploit commercial supply chains for the acquisition or diversion of sensitive goods and technologies.

Practical Compliance Measures for Economic Operators and Financial Institutions

In order to ensure effective implementation of sanctions and export control obligations, economic operators and financial institutions should complement regulatory compliance with practical, risk-based measures integrated into their day-to-day operations.

Economic operators should consider implementing the following measures:

- systematic screening of business partners and transactions against relevant sanctions and restricted party lists;
- verification of beneficial ownership structures in order to identify potential indirect links to sanctioned entities;
- monitoring of trade routes, transit countries and logistics arrangements, with particular attention to unusual or complex shipping patterns;
- establishment of internal reporting and escalation mechanisms for suspicious transactions or compliance concerns;
- regular staff training on export control requirements, sanctions regimes and risk indicators.

Financial institutions, given their central role in facilitating cross-border transactions, should additionally:

- monitor transaction flows for indicators of trade-based money laundering and proliferation financing;
- apply enhanced due diligence measures for high-risk clients, sectors or jurisdictions;
- ensure timely reporting of suspicious activities to competent authorities in accordance with applicable legal requirements.

The integration of these practical measures contributes to the development of a proactive compliance culture, reducing the risk of inadvertent involvement in illicit procurement networks and strengthening the overall effectiveness of the national control system.[8]

Common Red Flag Indicators for ACW-Related Transactions

The following indicators may suggest an increased risk of sanctions evasion, illicit procurement or diversion of dual-use goods, ACW components or sensitive technologies:

[8] https://documents1.worldbank.org/curated/en/850061468779087644/pdf/31477.pdf
https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Countering-Proliferation-Financing.pdf.coredownload.pdf

Customer-related indicators

- the identity of the customer or beneficial owner is unclear;
- the customer has little or no relevant business background;
- the customer's activity is inconsistent with the type or technical level of goods requested;
- the customer or its address matches, resembles or is linked to a sanctioned entity;
- the customer is reluctant to provide information on the end-user or end-use;
- the customer is evasive when asked whether the goods are intended for domestic use, export or re-export.

Goods-related indicators

- the requested goods exceed the apparent technical needs of the customer;
- the product's capabilities do not correspond to the buyer's declared activity;
- sensitive components are ordered in unusual quantities or combinations;
- the goods may be used in military, aerospace, UAV, communications, navigation or surveillance systems.

Shipping and logistics indicators

- the shipping route is unusual for the product or destination;
- goods are routed through intermediary jurisdictions without clear commercial justification;
- the freight forwarder, warehouse or logistics company is listed as the final destination;
- delivery dates or destinations are vague, inconsistent or frequently changed;
- packaging, labelling or shipping instructions are inconsistent with standard commercial practice.

Documentation and payment indicators

- invoices, end-user certificates or customs declarations contain inconsistencies;
- the declared end-use is vague, incomplete or not commercially plausible;
- payment is made by a third party not clearly connected to the transaction;
- payments originate from or are routed through jurisdictions associated with sanctions evasion or transshipment risks.

The presence of one or more red flags does not automatically confirm illicit activity. However, such indicators should trigger enhanced due diligence, additional verification and, where appropriate, consultation with competent authorities.

Key Recommendations for Economic Operators in the Republic of Moldova

In the context of evolving sanctions regimes, export control requirements and proliferation risks, economic operators in the Republic of Moldova should adopt a proactive and risk-based approach to compliance. The following recommendations are designed to support practical implementation and enhance resilience against illicit procurement and diversion risks.

1. Integrate sanctions screening and export control compliance into core business processes

Operators should ensure that sanctions screening, dual-use classification and licensing checks are embedded into procurement, sales and logistics workflows. This includes systematic verification of counterparties against relevant sanctions lists (UN, EU and national) and alignment with export control obligations under Regulation (EU) 2021/821 and national legislation.

2. Apply enhanced due diligence for high-risk transactions and jurisdictions Particular attention should be given to transactions involving:

- complex or multi-layered supply chains;
- intermediaries or newly established entities;
- jurisdictions associated with sanctions evasion or transshipment risks.

Enhanced due diligence should include verification of beneficial ownership, business activities and consistency between declared and actual end-use.[9]

3. Strengthen end-use and end-user verification mechanisms

Operators should go beyond formal documentation and assess the plausibility of the declared end-use. Red flags may include:

- discrepancies between goods and customer profile;
- reluctance to provide end-user information;
- unusual technical specifications or requests.

Where risks are identified, operators should suspend the transaction and seek guidance from competent authorities.[10]

4. Strengthen Client Onboarding and Continuous Due Diligence

Economic operators should integrate sanctions and export control questions into client onboarding procedures and throughout the business relationship. This should include verification of the customer's business profile, beneficial ownership, trading partners, previous transaction history and potential links to high-risk sectors or jurisdictions.

Particular attention should be given to clients involved in the manufacture, trade, transport or financing of defence-related items, electronics, microelectronics, aerospace components, UAV-related goods or other sensitive technologies.

[9] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.inline.pdf

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&rid=8

Due diligence should not be limited to the initial stage of the relationship. Operators should continuously monitor transactions, changes in ownership, unusual purchasing patterns, new shipping routes and repeated requests for re-export or transshipment.

Where inconsistencies or risk indicators are identified, the transaction should be suspended until additional verification is completed and, where necessary, guidance is obtained from competent authorities.

5. Monitor trade routes and logistics patterns

Given Moldova's position as a transit country and the presence of areas with limited regulatory oversight, operators should closely monitor shipping routes, transit countries and logistics arrangements. Particular caution is required in cases involving re-export, indirect routing or storage in intermediary locations, which may indicate diversion risks.[11]

6. Implement and continuously update Internal Compliance Programs (ICP)

A structured ICP should include:

- internal policies and procedures;
- clear allocation of compliance responsibilities;
- regular staff training;
- internal audit and monitoring mechanisms.

ICP frameworks should be adapted to the specific risk profile of the operator and regularly updated to reflect changes in sanctions regimes and trade patterns.

7. Incorporate virtual asset-related risks into compliance frameworks

With the increasing use of cryptocurrencies and digital payment systems, operators—particularly financial institutions—should integrate controls addressing virtual asset risks. This includes monitoring for unusual transaction patterns and ensuring alignment with AML/CFT standards on proliferation financing.

8. Promote a culture of compliance and proactive risk reporting

Compliance should not be treated as a formal requirement, but as an integral part of corporate governance. Operators are encouraged to establish internal reporting channels, promote awareness among employees and maintain open communication with competent authorities in case of suspicious activities or uncertainties.

[11] https://documents1.worldbank.org/curated/en/850061468779087644/pdf/31477.pdf

Enforcement Measures and Liability in Strategic Trade Control

The enforcement framework within the strategic trade control system of the Republic of Moldova ensures compliance through a combination of administrative (contravention), criminal and civil liability mechanisms. This multi-layered approach reflects the significant risks associated with unauthorized transfers of strategic goods, including dual-use items and other controlled technologies.

Administrative liability applies to violations of regulatory and licensing requirements, such as conducting export, import, re-export or transit operations without the required authorization, breaching licensing conditions, or failing to comply with reporting and record-keeping obligations. These infringements are governed by the Contravention Code of the Republic of Moldova, including provisions such as Art. 287, Art. 263–264 and Art. 330^{2}, and may result in fines, suspension of activities or withdrawal of licenses.

Criminal liability applies to serious offenses that threaten national or international security, including illegal export, re-export, transit or trafficking of strategic goods, as well as falsification of documentation or deliberate circumvention of control measures. Relevant provisions of the Criminal Code include Art. 248, Art. 248^{1}, Art. 249, Art. 290 and Art. 181^{1}, with sanctions ranging from fines and confiscation of assets to imprisonment.

Civil liability may arise where violations cause material damage to the state or private entities, requiring compensation under general civil law principles.

Enforcement measures also include preventive administrative actions, such as suspension or revocation of licenses, enhanced inspections and inclusion of operators in risk monitoring systems. These measures aim to prevent violations and strengthen compliance practices.

Effective enforcement relies on institutional coordination between customs, security and law enforcement authorities, as well as financial intelligence units. Given the transnational nature of strategic goods trafficking and sanctions evasion, international cooperation mechanisms, including information exchange and mutual legal assistance, remain essential.

Annex I. List of common high priority items

Statistical Assessment of Trade flows by Tier Classification (2021–2025) in the Republic of Moldova Based

This annex presents a comparative statistical overview of trade flows of the Republic of Moldova for selected goods corresponding to the Tier classification framework. The analysis is based on aggregated data expressed in quantity (units) and covers two reference periods: 2021 (baseline period) and 2025 (subsequent period).

The data reflects national trade statistics, aggregated based on selected HS codes corresponding, for analytical purposes, to the identified Tier categories.

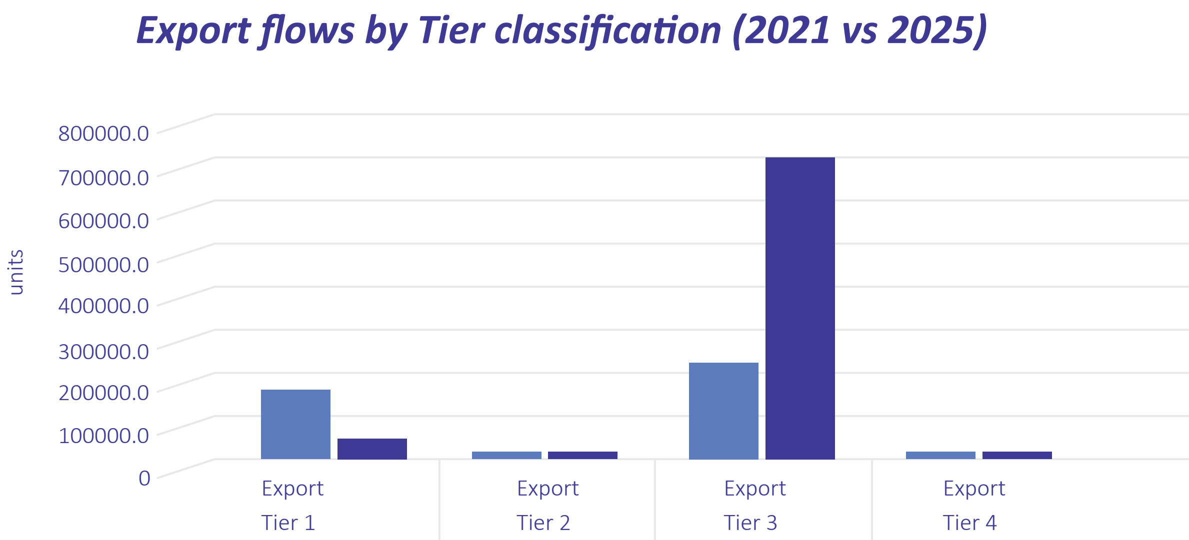
Classification of High-Priority Items (Tier 1–4):

For the purpose of this analysis, goods are grouped into four priority tiers based on international export control practice, particularly as reflected in guidance developed by the U.S. Bureau of Industry and Security (BIS) in coordination with partners such as the European Union and the United Kingdom.

Tier 1	Tier 2	Tier 1	Tier 4
includes the most sensitive and critical items, such as advanced semiconductors, integrated circuits, and other high-technology components with direct relevance for military, industrial, or dual-use applications.	covers important industrial and technological goods that support the functioning or production of higher-tier items, including certain electronic components, communication equipment, and manufacturing inputs.	comprises lower-sensitivity goods with potential indirect or supporting applications in industrial or technological processes.	includes goods with more limited strategic relevance, often representing general-purpose or widely available items that may still contribute to broader supply chains.

Figure 1 illustrates the distribution of export flows of the Republic of Moldova by Tier classification for the years 2021 and 2025, expressed in quantity (units). The data indicates an overall increase in export volumes, from 288,678 units in 2021 to 773,229 units in 2025. A decrease is observed in Tier 1 goods, from 105,233 units to 20,109 units. In contrast, Tier 2 exports increased from 3,842 to 7,980 units. The most significant growth is recorded in Tier 3 goods, which rose from 178,551 units in 2021 to 738,749 units in 2025, representing the largest share of export flows in the latter period. Tier 4 goods also show an increase, from 1,052 to 6,391 units, although their overall contribution remains comparatively limited.

[12] https://www.bis.gov/node/18319



	Export Tier 1	Export Tier 2	Export Tier 3	Export Tier 4
2021	105,233	3,842	178,551	1,052
2025	20,109	7,980	738,749	6,391

Figure 1. Export flows by Tier classification (2021 vs 2025)

Figure 2 presents the distribution of import flows of the Republic of Moldova by Tier classification for the years 2021 and 2025, expressed in quantity (units). The data shows a significant decrease in total import volumes, from 29,192,612 units in 2021 to 3,529,558 units in 2025. Tier 1 imports increased from 1,962,568 units to 3,114,569 units during the same period. Tier 2 imports decreased from 589,828 units in 2021 to 414,989 units in 2025. No import volumes are recorded for Tier 3 and Tier 4 goods in 2025, compared to 26,553,860 units and 86,356 units respectively in 2021.

Together, Figures 1 and 2 provide a comparative overview of the distribution of export and import flows across Tier classifications for the selected reference periods.

	Import Tier 1	Import Tier 2	Import Tier 3	Import Tier 4
2021	1,962,568	589,828	26,553,860	86,356
2025	3,114,569	414,989	0	0

Figure 2. Import flows by Tier classification (2021 vs 2025)

The Tier classification applied in this analysis is based on the framework developed by the Bureau of Industry and Security for identifying high-priority goods with potential relevance for advanced industrial and technological applications.

The statistical data presented in this annex reflects national trade flows of the Republic of Moldova and has been aggregated based on selected HS codes corresponding, for analytical purposes, to the identified Tier categories.

The mapping between HS codes and Tier classifications has been conducted exclusively for statistical and analytical purposes and does not constitute a legal classification of goods under national or international export control regimes.

The data is expressed in quantity (units) and is intended to support comparative analysis of trade patterns between the reference periods 2021 and 2025.

Any interpretation of the data should take into account potential limitations related to statistical aggregation, classification methodologies, and the evolving nature of international trade flows.

Disclaimer & source:

The statistical data presented in this analysis is compiled based on Harmonized System (HS) tariff codes and does not exclusively represent goods legally classified as dual-use or controlled items. It is widely acknowledged that not all tariff subheadings included in these categories correspond strictly to controlled goods under export control regimes. Therefore, the data should be interpreted as a general indicator of trade trends rather than a precise measurement of flows involving strategic or dual-use goods. The analysis relies on national trade statistics and customs data of the Republic of Moldova, complemented by publicly available international datasets, including UN Comtrade, as well as relevant analytical reports.

Annex II. Case Studies:

1. Attempted Smuggling of Components for Armoured Tracked Vehicles

In June 2019, Moldovan law enforcement authorities identified an attempted smuggling operation involving components intended for use in tracked armoured vehicles of the MT-LB type.

The case concerned a shipment of 47 double drive sprockets, which are essential elements of the transmission and running system of such military vehicles. The components were allegedly transported clandestinely from the administrative- territorial units located on the left bank of the Nistru River and temporarily stored within the territory of the Republic of Moldova.

According to the investigation, the goods were subsequently loaded into a cargo vehicle registered in the Republic of Moldova and were intended to be exported to the Russian Federation. In order to conceal the nature of the goods, the individuals involved declared them in customs documents as "agricultural machinery parts".

The attempted operation was intercepted at the Leușeni customs post, where the shipment was identified and seized by the competent authorities. The estimated value of the goods was approximately 764,000 MDL. The items were classified as strategic or military-related components and were subsequently placed under seizure and transferred for storage to the National Army's Armament and Ammunition Centre.

The case resulted in criminal proceedings against the individuals involved, in accordance with applicable legal provisions, which provide for penalties including imprisonment and sanctions against legal entities.

From a compliance perspective, this case illustrates several critical risk factors. First, it demonstrates the attempted diversion of military-related components through misdeclaration and concealment. Second, it highlights the use of indirect routes and storage locations prior to export. Third, it underscores the risks associated with transactions involving sensitive goods originating from areas with limited regulatory oversight.

Overall, the case provides a practical example of how illicit procurement and trafficking schemes may operate in the context of ACW-related supply chains, reinforcing the importance of effective customs control, accurate classification of goods and enhanced due diligence.[13]

[13] Customs data, https://www.jurnal.md/ro/news/cf9f5735961b4a2c/un-lot-de-piese-militare-estimat-la-circa-764-000-de-lei-ridicat-la-vama-leuseni-trei-indivizi-trimisi-in-judecata.html

2. Intermediary-Based Procurement Networks Involving Moldovan Entities

In the period 2022–2024, several companies registered in the Republic of Moldova were identified in investigative reporting and subsequently designated under international sanctions frameworks in connection with the supply of aviation-related components to entities located in the Russian Federation.

According to publicly available information, these companies operated as intermediaries (brokers), facilitating cross-border transactions involving aircraft parts through indirect procurement channels and complex supply chain arrangements. The transactions were identified through analysis of customs data and international trade databases, which indicated deliveries to Russian aviation-related entities following the introduction of Western restrictive measures.

In June 2024, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), designated several Moldovan-registered entities — including AEROSTAGE SERVICES SRL, AIRROCK SOLUTIONS SRL and MAX JET SERVICE SRL — under its Russia-related sanctions program. These designations resulted in the inclusion of the entities in the Specially Designated Nationals (SDN) List, triggering asset freezes and restrictions on access to the international financial system.

Subsequently, in August 2024, Moldovan authorities took administrative measures affecting the activity of these companies, following a review conducted within the framework of national mechanisms responsible for the monitoring of investment projects and economic security considerations.

From an analytical and compliance perspective, this case illustrates several important risk factors. First, it demonstrates how intermediary entities operating in third-country jurisdictions may be used to facilitate indirect trade with sanctioned destinations. Second, it highlights the challenges associated with identifying the ultimate end-user and end-use of goods in complex, multi-layered supply chains. Third, it underscores the potential gap between formal compliance with domestic legal provisions and broader alignment with evolving international sanctions regimes.

These findings reinforce the importance of implementing enhanced due diligence measures, including the verification of beneficial ownership, end-user identification, transaction monitoring and risk-based assessment of trade routes and counterparties. The case further illustrates the need for economic operators and financial institutions to adopt a proactive compliance approach that goes beyond minimum legal requirements and reflects international best practices in sanctions and export control compliance.[14]

[14] https://moldova.europalibera.org/a/companii-moldovene-au-livrat-piese-de-avion-in-rusia-in-ciuda-sanctiunilor-occidentale-/32799642.html , https://ofac.treasury.gov/recent-actions/20240612 , https://romania.europalibera.org/a/moldova-suspenda-companiile-care-au-intermediat-vanzarea-unor-piese-pentru-avioane-catre-/33077124.html

3. Illicit Trafficking and Concealment of Military Goods – Relevance for ACW Procurement Risks

A recent case (2025) detected at the Leușeni–Albița border crossing point involved the attempted smuggling of military-grade equipment, including weapons systems and related components, which were falsely declared in customs documentation as "metal parts". The investigation revealed elements of a coordinated transnational network, involving intermediaries, logistical support chains, and cross-border transport arrangements.

Although the case primarily concerned complete conventional weapons rather than individual high-tech components, it provides a relevant illustration of illicit transaction patterns applicable to the procurement of Advanced Conventional Weapons (ACW) components and other sensitive technologies. In particular, the case highlights:

- the use of falsified declarations and misclassification of goods to evade detection;
- the role of intermediaries and fragmented supply chains in facilitating illicit procurement;
- the application of covert transshipment techniques, including concealment of the true nature and destination of goods;
- the exposure of transit countries, such as the Republic of Moldova, to diversion and trafficking risks.

These patterns are equally relevant in the context of ACW-related supply chains, where sensitive components (e.g. electronics, guidance systems, or specialized materials) may be trafficked using similar concealment methods. The case therefore serves as an operational example of how illicit procurement networks can function across different categories of controlled or sensitive goods, including both complete weapons systems and their underlying components.[15]

[15] https://www.zdg.md/stiri/cazul-contrabandei-cu-armament-de-la-leuseni-albita-cinci-persoane-aflate-in-arest-preventiv-la-ce-etapa-se-afla-dosarul-penal/

Annex III. Practical Compliance and Risk-Check List for Controlled or Sensitive Goods Transactions

This checklist is intended to support both economic operators and relevant authorities (e.g. customs, law enforcement, financial intelligence units, licensing authorities) in identifying, assessing and preventing illicit transactions involving controlled goods, including components related to Advanced Conventional Weapons (ACW) and other sensitive technologies

A. Product and Classification Control

- ☐ Is the item correctly identified (technical description, specifications, functionality)?
- ☐ Verify whether the goods, software or technology are listed under:
  - EU Dual-Use Control List (Annex I of Regulation (EU) 2021/821)
  - National control lists (DU/ML list) (GD no.24/2025)
- ☐ Determine the correct HS code and dual-use classification
- ☐ Assess whether the item falls under high-priority or restricted categories
- ☐ Check for catch-all controls (non-listed items with potential military/end-use risk)

B. End-User and End-Use Verification

- ☐ Identify the final end-user and obtain complete details (name, address, business activity)
- ☐ Request and verify an End-User Certificate (EUC)
- ☐ Assess the intended end-use of the goods
- ☐ Screen for risks of:
  - Military end-use
  - Use in weapons of mass destruction (WMD)
  - Diversion or re-export to sanctioned destinations

C. Sanctions and Restricted Party Screening

- ☐ Screen all parties involved (buyer, consignee, intermediary) against:
  - EU sanctions lists
  - UN sanctions lists
  - National restricted party lists
- ☐ Verify whether the destination country is subject to:
  - Embargoes
  - Sectoral sanctions
- ☐ Ensure no involvement of sanctioned entities or individuals

D. Licensing Requirements

- ☐ Determine whether an export license is required
- ☐ Identify the appropriate type of license:
  - Individual license

- Global license
- General authorization

- ☐ Prepare and submit complete documentation to the competent authority
- ☐ Ensure compliance with license conditions and validity

E. Internal Compliance Program (ICP) Measures

- ☐ Establish written export control policies and procedures
- ☐ Assign a compliance officer or responsible unit
- ☐ Provide regular staff training on export control obligations
- ☐ Maintain internal screening and risk assessment procedures
- ☐ Implement record-keeping systems (minimum retention period as required by law)

F. Transaction and Logistics Control

- ☐ Verify consistency between:
  - Commercial invoice
  - Transport documents
  - Customs declarations
- ☐ Monitor shipping routes and transit countries
- ☐ Identify unusual or suspicious shipping arrangements
- ☐ Ensure accurate declaration to customs authorities

G. Red Flags and Risk Indicators

- ☐ Customer unwilling to provide end-use information
- ☐ Inconsistencies in documentation or transaction details
- ☐ Unusual routing or third-country intermediaries
- ☐ Products not matching the customer's business profile
- ☐ Requests for unnecessary technical specifications or modifications

H. Post-Export Compliance

- ☐ Maintain records of all export transactions
- ☐ Monitor compliance with license conditions
- ☐ Report suspicious activities to competent authorities
- ☐ Conduct internal audits and compliance reviews

Annex IV. Useful links

This annex provides key institutional, legal and informational resources relevant to export control and international sanctions.

A. European Union Resources:

European Commission – Dual-Use Export Controls

https://policy.trade.ec.europa.eu

EUR-Lex – Regulation (EU) 2021/821 (Dual-Use Regulation)

https://eur-lex.europa.eu

EU Sanctions Map

https://www.sanctionsmap.eu

B. International Organizations:

United Nations Security Council Sanctions Committees

https://www.un.org/securitycouncil/sanctions

Wassenaar Arrangement

https://www.wassenaar.org

Missile Technology Control Regime (MTCR)

https://mtcr.info

Nuclear Suppliers Group (NSG)

https://www.nuclearsuppliersgroup.org

Australia Group

https://www.australiagroup.net

Bureau of Industry and Security (BIS) – U.S. Department of Commerce

https://www.bis.doc.gov

Consolidated Screening List

https://www.trade.gov/consolidated-screening-list

C. National links:

Customs Commercial Information Portal

https://trade.gov.md/ro

Law No. 213 of 31 July 2024 on the Control of Trade in Strategic Goods
https://www.legis.md/cautare/getResults?doc_id=144745&lang=ro

Government Decision No. 24/2025 on the National System for the Control of Trade in Strategic Goods in the Republic of Moldova
https://www.legis.md/cautare/getResults?doc_id=147737&lang=ro

Law No. 25/2016 on the Implementation of International Restrictive Measures
https://www.legis.md/cautare/getResults?doc_id=149779&lang=ro

D. Compliance and Guidance Materials:

EU Guidance on Internal Compliance Programs (ICP)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318

OECD Guidelines on Due Diligence

https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/oecd-due-diligence-guidance-for-responsible-business-conduct_c669bd57/15f5f4b3-en.pdf

FATF Guidance on Proliferation Financing

https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

UN Comtrade Database

https://comtradeplus.un.org/TradeFlow