SECTOR-SPECIFIC RISK ANALYSIS

FINANCING OF PROLIFERATION

2025

MINISTERIO
DE ECONOMÍA, COMERCIO
Y EMPRESA

COMISIÓN DE PREVENCIÓN DEL
BLANQUEO DE CAPITALES E
INFRACCIONES MONETARIAS

Contents

1. Executive Summary 4
2. Introduction 7
2.1 Presentation 7
2.2 Objectives 8
3. Methodology 10
3.1. Participating Institutions 10
3.2. Sources of Information 11
3.3. Definitions and Methodology 11
4. Institutional framework on proliferation 14
4.1. International Instruments 14
4.1.1 International instruments with jurisdiction over proliferation financing in which Spain participates. 14
4.1.2. International organizations with jurisdiction over proliferation in which Spain participates 15
4.1.3. International treaties and commitments signed by Spain regarding proliferation 17
4.2. National structure 17
4.3. Spain's diplomatic relations with the DPRK and Iran 19
5. Key Threats to Proliferation Financing 20
5.1. Threats at the international level 20
5.2. Threats identified at the national level 23
5.3. Emerging threats 27
6. Key Vulnerabilities 29
6.1. Structural Vulnerabilities 29
6.1.1. Stemming from the regulatory framework 29
6.1.2. Stemming from the implementation of UNSC sanctions 29
6.1.3. Arising from the absence of a National Coordinating Authority on Proliferation Financing 30
6.1.4. Derived from compliance by the private sector 30
6.2. Contextual or Geographical Vulnerabilities 31
6.3. Sectoral vulnerabilities 31
6. 3.1. Arising from international trade 31

6. 3.2. Derived from the financial sector 33
6. 3.3. Derived from non-financial activities and professions 34
6.4. Specific vulnerabilities of marketed products and services 34
6.5. Summary of vulnerabilities 37
7. Risks 42
7.1. Inherent Risks 42
7.2. Mitigation measures 44
7.2.1. Institutional Mitigation Measures 44
7.2.2. Commercial mitigation measures 46
7.2.3. Beneficial ownership control mechanisms to prevent the provision of assets to sanctioned persons 47
7.2.4. Measures implemented by the financial sector 48
7.3. Residual risk 49
APPENDIX 1—Export Control Statistics 51
APPENDIX 2. Legal framework governing the marketing of dual-use goods use 56
ACRONYMS 57

1. Executive Summary

The financing of the proliferation (hereinafter, PF) of weapons of mass destruction (hereinafter WMD) is significant due to the mobilization of funds and the introduction into the international financial system of illicit funds used for the manufacture, acquisition, or transport of sanctioned goods or the development of nuclear weapons.

PF of WMD is a constantly evolving international challenge against which measures are being established by various organizations. On the one hand, the United Nations, through resolutions issued by the Security Council (hereinafter, UNSC), and on the other, the Financial Action Task Force (hereinafter FATF), by establishing PF of WMD as a third pillar to be addressed from a preventive perspective. Obligations in this area are primarily set forth in Recommendation 7 of the FATF standards, though it should be noted that Recommendation 1 establishes the need to assess money laundering risk and Recommendation 2 emphasizes international cooperation in this area. The effectiveness of compliance with money laundering obligations is assessed in Immediate Outcome 11.

The overall objective of this sectoral risk analysis is to identify and understand the threats, vulnerabilities, and risks facing vocational training in Spain. All relevant stakeholders, from both the public and private sectors, participated in this analysis.

The analysis is based on quantitative and qualitative information, drawn from the review of strategic documents, reports, and official statistics. Additionally, a working group was established with Spain's leading banking institutions, with whom we engaged during the preparation of this report and discussed the main topics addressed. Following this working group, a questionnaire was distributed to identify the threats, vulnerabilities, and key mitigation measures currently in place within our financial system.

To determine risk exposure, we analysed evidence related to jurisdictions directly linked to PF (the Democratic People's Republic of Korea and Iran), as well as evidence arising from interactions with other intermediary jurisdictions. Taking these factors into account, within the national framework, threats focus on cybercrimes carried out by organizations operating on a global scale, international transfers involving intermediate jurisdictions considered high-risk, and international commercial activity in which threats of diversion of defense materials and prohibited chemical substances to intermediate high-risk jurisdictions via shell companies, and payment settlement activities on behalf of Iranian companies that may be linked to Iran's nuclear or missile programs.

The illicit financial activity generated through proliferation plays a significant role in the movement of funds destined for or originating from the PF. In this regard, the use of shell companies and links to intermediary jurisdictions are the primary threats

identified.

The vulnerabilities that can be exploited by these threats stem primarily from Spain's geostrategic position as a meeting point of three continents and its location on one of the world's major maritime routes, namely the Strait of Gibraltar.

On the other hand, detecting suspicious activity indirectly linked to PF poses difficulties given the interconnection with other criminal activities related to money laundering and terrorist financing (hereinafter ML/TF).

Following an analysis of the threats and vulnerabilities affecting the national context regarding PF of WMD proliferation, it has been concluded that the inherent risk is medium-low.

Existing mitigation measures reduce the initial risk. These include, notably: the absence of cooperation projects between Spain and the Democratic People's Republic of Korea (hereinafter, DPRK or North Korea), the legal basis for enforcing financial sanctions through European Union (EU) Regulations, both the DPRK regime and the application of the amendment to Regulation (EU) No. 267/2012 with the strengthening of measures against the Iranian nuclear program following the "snap-back" of sanctions in 2025. Likewise, the report highlights as mitigation measures the Spanish sector-specific regulations based on the nature of the manufacturing of each type of dual-use material, existing regulations on international trade, mechanisms for controlling beneficial ownership, and the financial system's transaction alert and detection systems, as well as the automated procedures implemented for the enforcement of sanctions.

The sectors most exposed to risk are those related to correspondent banking, credit institutions and electronic money institutions, and crypto-asset service providers. There is no evidence in Spain indicating the existence of natural channels of exposure to PF in non-financial sectors; therefore, the risk is initially assessed as very low.

In conclusion, after adjusting for the inherent risk level based on existing mitigation measures, it has been determined that the residual risk regarding PF of WMD is low.

2. Introduction

2.1 Overview

WMD financing encompasses the money or financial resources used to support the manufacture, acquisition, transport, or development of nuclear, chemical, and biological weapons, as well as the means to deliver them.

On the one hand, the United Nations aims to address the proliferation of WMDs through resolutions issued by the UNSC. On the other hand, from a financial perspective, the FATF has strengthened existing requirements regarding PF, making them the third pillar of its preventive objectives, alongside the prevention of money laundering and terrorist financing (hereinafter, AML/FT).

The FATF's obligations regarding non-proliferation are set forth in Recommendation 7, which requires countries to:

- Freeze funds or other assets without delay and ensure that no funds or other assets are made available, directly or indirectly.

- Establish mechanisms to communicate designations to financial institutions and designated non-financial businesses and professions (hereinafter, DNFBPs).

- Require financial institutions and DNFBPs to report to the competent authorities any frozen assets or actions taken in compliance with the prohibitions set forth in relevant Security Council resolutions, including attempted transactions.

- Take appropriate measures to monitor and ensure compliance with the obligations set forth in Recommendation 7 by financial institutions and DNFBPs.

None of the requirements of Recommendation 7 are intended to replace other measures or obligations that may already be in place for handling funds or other assets in the context of a criminal, civil, or administrative investigation or proceeding.

The emphasis of Recommendation 7 is on preventive measures. These are necessary and unique in the context of stopping and preventing the flow of funds or other assets to proliferators or for proliferation.

Recommendation 7 applies to all current UNSC resolutions imposing targeted financial sanctions in the context of PF of WMD, as well as to any future successor resolutions establishing targeted financial sanctions.

On the one hand, with regard to the DPRK, Resolution 1718 (2006) and its subsequent resolutions—1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), and 2356 (2017).

On the other hand, with regard to Iran, Resolutions 1737 (2006), 1747 (2007), 1803 (2008), and 1929 (2010) apply, which imposed sanctions related to its nuclear program. These sanctions were largely lifted following Iran's accession to the Joint Comprehensive Plan of Action in 2015 (hereinafter JCPOA) and the subsequent adoption of Resolution 2231 (2015), which endorsed the agreement. This Resolution established a "snap-back" mechanism to reimpose sanctions in the event of non-compliance. In September 2025, the UNSC failed to adopt a resolution extending the sanctions relief under the JCPOA, meaning that the lifted sanctions are automatically reimposed unless a new resolution is adopted within the established mechanism.

It should be noted that there have recently been changes to the FATF standards related to PF for the Fifth Round of evaluations, aimed at improving understanding of the risks and enhancing coordination. In particular, Recommendation 1 was updated to require that countries and private-sector entities identify, assess, understand, and mitigate proliferation financing risks, emphasizing the need to implement risk-based measures to prevent potential breaches or circumvention of targeted financial sanctions. Additionally, Recommendation 2 was strengthened to improve national cooperation and coordination in the fight against PF of WMD.

2.2 Objectives

In 2020, a National Risk Analysis (hereinafter NRA) was prepared in Spain, analysing threats and vulnerabilities in the area of ML/FT, including a specific section on risks related to violations of international financial sanctions, both those related to CFT and PF.

The NRA was reviewed and updated in 2024 through the publication of an addendum that included a revision of this analysis. Notwithstanding the foregoing, it has been deemed necessary to delve deeper into the existing threats and vulnerabilities in the country regarding the risk of evasion and non-compliance with the implementation of financial sanctions related to PF.

Therefore, the overall objective of this document is to identify and understand the threats, vulnerabilities, and risks regarding the evasion of financial sanctions related to PF. This overall objective is accompanied by other specific objectives such as:

- Design an infographic to assist regulated entities in assessing, analysing, and determining non-proliferation risks, as well as to facilitate their compliance with their obligations in this area.
- Development of outreach programs on proliferation risks in our country to raise public awareness of the potential impact of sanctions evasion.
- Implementation of the Action Plan on Non-Proliferation, which provides for an ad hoc non-proliferation analysis.

3. Methodology

3.1. Participating Institutions

The public institutions involved in the preparation of this analysis were:

- Spanish Tax Administration Agency, Agencia Estatal de Administración Tributaria (hereinafter, AEAT);
- Banco de España.
- National Intelligence Centre, Centro Nacional de Inteligencia (hereinafter, CNI);
- Centre for Intelligence Against Terrorism and Organized Crime, Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (hereinafter, CITCO),
- General Information Directorate of Policía Nacional.
- General Council of the Judiciary, Consejo General del Poder Judicial (hereinafter, CGPJ).
- Department of National Security.
- Directorate-General for Foreign Policy and Security.
- Office of the Prosecutor General.
- Prosecutor's Office of the Audiencia Nacional.
- Special Prosecutor's Office for Corruption and Organised Crime.
- Information Directorate of Guardia Civil.
- Secretariat of State for Security.
- General Secretariat of the Treasury and International Finance.
- Executive Office of the Commission for the Prevention of Money Laundering and Monetary Offenses, Servicio Ejecutivo de Prevención de Blanqueo de Capitales (hereinafter, SEPBLAC).
- Subdirectorate General for International Trade in Defense and Dual-Use Equipment.

In addition, a working group was established with participants from the private sector, including representatives from the following institutions:

- Spanish Banking Association, Asociación Española de Banca (hereinafter, AEB).
- Banco Bilbao Vizcaya, S.A.
- Banco Santander, S.A.
- Banco de Crédito Social Cooperativo, S.A.
- CaixaBank, S.A.
- CecaBank, S.A.
- Deustche Bank, S.A.
- National Union of Credit Cooperatives, Unión Nacional de Cooperativas de Crédito

(hereinafter, UNACC).

3.2. Sources of information

The following documents have been taken into consideration:

- Spain's 2020 National Risk Assessment and the 2024 Addendum.
- 2022 Executive Guide on Non-Proliferation and Disarmament.
- 2021 National Security Strategy.
- CCN-CERT. Cyber Threats and Trends. 2024 Edition.
- FATF's 2024 Guidance on Money Laundering National Risk Assessment.
- 2021 FATF Guidance on Proliferation Financing Risk Assessment and Mitigation.
- Complex Proliferation Financing and Sanctions Evasion Schemes, FATF, 2025.
- Reports of Expert Groups established pursuant to the Resolutions.
- Consultations with the various competent authorities in each area of activity and documents prepared by them, some of which are classified.

3.3. Definitions and Methodology

The following are the definitions of the main concepts that will be used throughout this analysis:

- **Proliferation Financing**[1] is any act that **provides funds or uses financial services**, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fragmentation, transport, transfer, storage, or use of nuclear, chemical, or biological weapons, their means of delivery, and other related materials (including dual-use technologies and goods for illicit purposes) in **violation of national laws or** international **obligations**, where applicable.

Within this concept, a distinction must be made between:

a) **Direct financing:** involves the use of funds to **explicitly support proliferation activities**.

[1] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf

b) Indirect financing: refers to **unintentional or disguised financial support** that facilitates proliferation activities.

Based on these definitions, the methodology established in the *"FATF Guidance on the Assessment and Mitigation of Proliferation Financing* Risks" has been used. This guidance proposes combining the identification of the following factors:

(i) existing threats in Spain,
(ii) system vulnerabilities and the country context that allow these threats to carry out their activities, and
(iii) the sectors (economic and non-economic) and the types of entities and legal structures that may be used or exploited by these threats to carry out PF activities by taking advantage of existing vulnerabilities regarding the evasion of financial sanctions.

According to the FATF, when it defines **"threats"** to PF, it refers to *"designated persons and entities that have previously caused, or have the potential to cause, evasion, non-compliance, or exploitation of a failure in the implementation of AML-CFT measures in the past, present, or future. Such a threat may also be posed by persons or entities acting for or on behalf of designated persons or entities. It may be an actual or potential. Not all threats pose the same level of risk to all countries and private-sector companies."*

Given that these threats are criminal in nature and intended to destabilize society, their analysis must primarily take a law enforcement approach, based on an assessment by the authorities responsible for investigating and prosecuting criminal activities, such as law enforcement agencies (the Guardia Civil, the General Directorate of the Policía Nacional, or regional police forces), CITCO, the CNI, the Office of the Attorney General, judges and courts, or the AEAT in customs and tax matters.

For their part, **"vulnerabilities"** are those situations and circumstances *"that can be exploited by the threat or that can support or facilitate the violation, non-application, or evasion of the PF*."

An individualized analysis of the impact of these vulnerabilities involves a study of each of the different financial and non-financial sectors: their activities, corporate structures, and other elements and operations that could be exploited by various threats for money laundering purposes, leading to an assessment of the risk level for each sector.

In accordance with the rating system established in Article 12.3 of Regulation (EU) 2024/1620 of the European Parliament and of the Council of May 31, 2024, establishing the Anti-Money Laundering and Counter-Terrorism Authority, the levels of inherent and residual risk shall be rated as follows:

- Low
- Medium
- Substantial
- High

4. Institutional architecture on proliferation

4.1. International instruments

4.1.1 International instruments with jurisdiction over proliferation financing in which Spain participates.

United Nations

The UNSC takes a two-pronged approach to countering PF through resolutions adopted under Chapter VII of the UN Charter, which therefore impose obligations on UN Member States:

(i) **Comprehensive approach under UNSCR 1540 (2004) and its successor resolutions:**

This Resolution and its successors prohibit the financing of proliferation-related activities by non-state actors and require countries to establish, develop, review, and maintain adequate controls over the provision of funds and services, such as financing, related to the export and transshipment of items that could contribute to the proliferation of WMD.

The objective of this Resolution is to ensure that effective measures are taken to prevent the proliferation and use of WMD by non-state actors, particularly terrorist groups.

Following this resolution, the **1540 Committee** was established in 2004, comprising the 15 member states of the UN Security Council. Its purpose is to ensure that States refrain from providing any form of support to non-state actors seeking to develop, acquire, manufacture, possess, transport, transfer, or use nuclear, chemical, or biological weapons and their delivery systems.

(ii) **Country-specific approach:**

There are currently two UNSC sanctions regimes with a country-specific focus: the first is the one established by **Resolution 1718 (2006) and its subsequent** resolutions**, directed against North Korea** in response to its nuclear and ballistic missile tests, which impose a comprehensive arms embargo, as well as financial, trade, and transport restrictions.

The second pertains to **Resolution 1737 (2006) and its successor resolutions, which target Iran.** Although Resolution 2231 (2015), regarding Iran's reaffirmation of the JCPOA, suspended the UNSC financial sanctions imposed by Resolutions 1737 (2006), 1747 (2007), 1803 (2008), and 1929 (2010), while maintaining certain specific restrictions, on September 27, 2025, the UNSC decided to reinstate targeted sanctions. This was done in application of the so-called *"snap-back"* mechanism, provided for in Resolution 2231 itself, which entails the reimposition of the ban on transfers of arms and materials related to nuclear and ballistic missile programs, the asset freeze, and travel restrictions on individuals and entities linked to the regime, as well as financial and trade restrictions aimed at preventing direct or indirect support for its proliferation programs.

4.1.2. International organizations with jurisdiction over proliferation issues in which Spain participates

(i) United Nations.

In addition to the aforementioned resolutions, the UN has various institutions whose mission is to ensure global disarmament:

- Office for Disarmament Affairs (UNODA)
- Conference on Disarmament
- Disarmament Commission
- United Nations Institute for Disarmament Research (UNIDIR)

(ii) European Union

The European Union (hereinafter, *the* EU) has the *"EU Strategy against the Proliferation of* WMD" of 2003, which aims to integrate all available instruments within the EU to prevent and halt the proliferation of WMD. Non-proliferation measures are implemented primarily through two specific regimes:

- **Council Regulation (EU) No 267/2012 of March 23, 2012, concerning restrictive measures against Iran**, with particular reference to Decision (CFSP) 2025/1978, amending Decision 2010/413/CFSP, the purpose of which is the immediate reintroduction in the EU of all nuclear-related sanctions suspended

due to breaches of the JCPOA, as well as the other legal instruments adopted on September 29, 2025, amending Regulation (EU) No 267/2012.

- **Council Regulation (EU) 2017/1509 of August 30, 2017, concerning restrictive measures against the Democratic People's Republic of Korea**, which strengthens sanctions against that country by imposing a total arms embargo, export and import restrictions, financial limitations, travel bans, and asset freezes.

(iii) NATO

NATO has no direct legal authority to regulate or sanction the financing of proliferation, as the North Atlantic Treaty does not provide for functions in the financial or sanctions areas. However, its actions are indirectly grounded in Articles 4 and 5 of the Treaty, which allow it to address any threat to the security of member states, including the proliferation of weapons of mass destruction and the networks that finance it.

(iv) Organization for Security and Co-operation in Europe (OSCE)

There is no specific treaty granting the OSCE authority over proliferation financing. Its role stems from political commitments that enable it to support the implementation of UN resolutions and strengthen the capacities of participating States, without having its own regulatory or sanctioning powers. Among these commitments, the 2003 Maastricht signing of the OSCE Strategy to Address Threats to Security and Stability in the 21st Century stands out; it recognizes the proliferation of WMDs and the networks that finance it as threats and commits states to cooperate to prevent them.

(v) Proliferation Security Initiative (PSI)

Launched in 2003, it seeks to prevent the illicit trafficking of WMD, their delivery systems, and related materials to and from states and non-state actors, with an

emphasis on the interception of illicit traffic. It comprises a core group of 23 participating countries that meet annually within the so-called Group of Operational Experts and serves as a forum for discussing and developing concepts to improve member states' capabilities in the legal and operational spheres.

4.1.3. International treaties and commitments signed by Spain regarding proliferation

Spain has ratified various international treaties and commitments regarding nuclear weapons, chemical weapons, and biological weapons:

(i) Treaty on the Non-Proliferation of Nuclear Weapons (NPT).
(ii) Treaty on the Prohibition of Nuclear Weapons (TPNW).
(iii) Comprehensive Nuclear-Test-Ban Treaty (CTBT).
(iv) Fissile Material Cut-off Treaty (FMCT).
(v) Stockholm Initiative on Nuclear Disarmament.
(vi) Global Initiative to Combat Nuclear Terrorism (GICT).
(vii) Group of Nuclear Suppliers (GNS).
(viii) Chemical Weapons Convention (CWC).
(ix) Organization for the Prohibition of Chemical Weapons (OPCW) International Partnership Against Impunity for the Use of Chemical Weapons.
(x) Convention on Biological and Toxin Weapons (BTWC).
(xi) Secretary-General's Mechanism for Investigating Alleged Use of Chemical, Biological, or Toxin Weapons (UNSGM).

4.2. National Structure

4.2.1 Institutional Architecture for Non-Proliferation

In the area of non-proliferation, two important bodies with national-level authority stand out:

On the one hand, **the Specialized Committee on Non-Proliferation,** established by Order PRA/29/2018 of January 22, which publishes the Agreement of the National Security Council establishing and regulating the Specialized Committee on the Non-Proliferation of Weapons of Mass Destruction. It is a body that supports the National

Security Council, as provided for in Article 20.3 of Law 36/2015 of September 28 on National Security, and is responsible for carrying out the functions assigned by the Council in the field of WMD non-proliferation and within the framework of the National Security System.

On the other hand, the **Interministerial Regulatory Board for Foreign Trade in Defense and Dual-Use Materials, Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso** (**Hereinafter, JIMDDU)**[2]. It is the highest national body responsible for evaluating operations related to foreign trade in defense and dual-use materials, and is chaired by the Secretary of State for Trade. The JIMDDU plays an essential role in this area, as it is responsible for issuing mandatory and binding administrative authorizations for transfers of defense equipment, other equipment[3],and dual-use products and technologies.

4.2.2 Institutional architecture and regulatory framework regarding proliferation financing

The Specialized Committee on WMD Non-Proliferation, at its meeting on July 20, 2022, approved the creation of **the Working Group on Proliferation Financing,** regarding the new obligations imposed by the FATF on PF.

In July 2024, it submitted a draft National Plan against the Financing of the Proliferation of WMD. This was submitted to the Non-Proliferation Committee for review and approval at its meeting on April 23, 2025. Subsequently, the National Security Council did the same on July 14, 2025, and the plan was submitted to the Council of Ministers. Finally, the Plan was published in the Official State Gazette (Boletín Oficial del Estado, BOE) as Order PJC/1028/2025, dated September 10, publishing the Agreement of the Council of Ministers of August 26, 2025, approving the National Plan against the Financing of the Proliferation of Weapons of Mass Destruction.

With regard to the regulatory framework for the financing of proliferation, Article 42 of Law 10/2010 of April 28 on the prevention of money laundering and the financing of terrorism includes specific provisions to ensure the enforcement of international financial sanctions. These are supplemented by the implementing regulations

[2] Established by Law 53/2007 of December 28 on the control of foreign trade in defense and dual-use materials. Section 3 of this Law regulates its structure and functions.

[3] Hunting and sporting weapons, police and riot control equipment, and instruments intended for torture and the death penalty

contained in Articles 47 through 49 of the Regulations of Law 10/2010 of April 28, approved by Royal Decree 304/2014 of May 5.

This framework is supplemented at the European level by the provisions of Regulation (EU) 2024/1624 of the European Parliament and of the Council of May 31, 2024, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

4.3. Spain's Diplomatic Relations with the DPRK and Iran

On December 15, 2000, the Council of Ministers gave the green light to the establishment of diplomatic relations with the DPRK. Spain has formally maintained diplomatic relations with Pyongyang since February 7, 2001, a decision adopted jointly with the rest of the EU Member States, except France.

Since 2006, relations have been managed under a multiple accreditation system through the Spanish Embassy in Seoul. North Korea opened a resident embassy in Madrid in October 2013 and closed it in October 2023. Currently, the DPRK Embassy in Rome is accredited to handle Spanish affairs.

In the case of Iran, Spain has maintained diplomatic relations with Iran since 1950. The Spanish Embassy in Tehran opened in 1951, consolidating bilateral diplomatic and consular channels. On the Iranian side, the Iranian Embassy in Madrid has been in operation since 1956, maintaining ongoing diplomatic activity.

Over the past few decades, the relationship has developed within the broader framework of the European Union's foreign policy toward Iran, particularly in areas such as political dialogue, economic cooperation, and the implementation of EU and United Nations sanctions regimes.

Currently, relations are conducted through both embassies (Spain in Tehran and Iran in Madrid), as well as through diplomatic and consular coordination within the EU. Although the bilateral relationship has gone through different phases of intensity due to the regional and international context, diplomatic channels remain open and operational, albeit with restrictions.

5. Key threats regarding proliferation financing

5.1. International-level threats

According to the FATF Guidance on Assessing and Mitigating Proliferation Financing Risk, the factors to be analysed regarding these threats focus on identifying designated persons or entities, the activities they carry out, and the ways in which they attempt to evade targeted financial sanctions**.**

The document *Complex Proliferation Financing and Sanctions Evasion Schemes* (FATF, June 2025)[4] mentions the main **aggravating factors for the DPRK's proliferation financing** and its WMD program: the DPRK's growing financial connectivity and the diversity of its revenue-generating sources.

Regarding the first factor, Russia is one of the key relevant actors. Specifically, in 2024, Russia signed the Comprehensive Strategic Partnership Treaty with the DPRK[5] .

As for the second factor—the diversification of revenue sources—cyberattacks and cryptoasset thefts have gained prominence.

The international threats associated with Iran focus on the use of sanctions-evasion networks that include oil smuggling, the use of money changers and foreign banks, as well as complex schemes involving shell companies and trust service providers that facilitate the concealment of beneficial ownership and the acquisition of dual-use goods.

[4] www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf
[5] http://en.kremlin.ru/acts/news/75534

Table 1. International PF of WMD threats

THREAT TYPE	DEVELOPMENT	EVIDENCE
System representatives	Typically representatives of the banking sector who act through financial allies in intermediary jurisdictions to move funds. Use of money changers in the United Arab Emirates and Türkiye, employing *hawala-style* schemes.	*DPRK: Sim Hyon Sop*, a representative of the *Korea Kwangson Banking Corporation* (KKBC), received over $24 million in crypto assets, half of which came from North Korean tech workers who, using false identities, secured jobs at tech companies (including U.S. firms) and demanded payment in virtual currencies. *Iran:* A network of currency exchange houses in Dubai that, acting on behalf of the Central Bank of Iran and the *IRGC-Qods Force*, processed revenues from oil exports and transferred them through foreign correspondent banks, thereby concealing their true origin and destination.
Shell companies and opaque corporate structures	Lack of transparency regarding beneficial ownership, a transnational nature that enables transactions in different currencies, and concealment of the true nature of the transactions. Triangulation in the purchase of dual-use materials through a front company in an intermediary third country and payment from a financial institution located in another third country. Identified high - risk intermediary countries:	*DPRK*: *Glocom* (Malaysia), a DPRK front company engaged in the covert sale of military communications equipment. *Stroytreyd LLC* (Moscow), identified in 2023–2024 as a front company to recover funds from bankrupt Russian banks and transfer them to the DPRK, with support from the *Russian Financial Corporation* and *Timer Bank*. *Iran*: *Shiraz Electronics Industries* (SEI) and *Rayan Roshd Afzar* are Iranian companies identified for developing missiles and drones. They are linked to the operations of four Chinese nationals

	Russia, Hong Kong, and the United Arab Emirates.	who used front companies in China to channel U.S.-origin dual-use items to these sanctioned entities.

Cyberattacks	Use of cryptoassets and decentralized finance (DeFi) platforms, such as mixers, unregulated exchanges, and anonymity tokens.	Lazarus Group. Use of ransomware such as Maui[6] and H0lyGh0st[7] .
Manipulation of maritime transport	Proliferation operation with financial impact. Ship-to-ship transfers on the high seas and the falsification of cargo documentation. Import of petroleum products that generate revenue through the illegal export of coal.	*DPRK*: Independent investigations by C4ADS[8]and reports from the U.S. Department of the Treasury. *Iran*: In 2021, a U.S. company forged export documents to divert components classified as dual-use goods to a high-risk country linked to Iran's nuclear program. Use of front companies, falsified documentation, and fraudulent import/export structures to conceal the true ownership and final destination of the goods.

Smuggling and trafficking of high-value goods	Activities associated to criminal organizations.	*DPRK*: The United Nations Panel of Experts (2024[9]) documented smuggling operations involving ivory and rhino horn originating from Africa; trafficking of methamphetamines and weapons light aircraft coordinated by representatives abroad, whose proceeds were funneled into the nuclear and missile programs. Iran: smuggling of oil, gold, and luxury goods through intermediaries in the United Arab Emirates, Türkiye, and East Asia (U.S. Department of the Treasury[10]).

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a

[7] https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

[8] C4ADS, Risky Business: A System-Level Examination of North Korea's Proliferation Financing and Sanctions Evasion Networks, 2019, https://c4ads.org/s/RiskyBusiness.pdf

[9]https://docs.un.org/en/S/2024/215

5.2. Threats detected at the national level

In the case of Spain, information provided by the public and private sectors regarding threats related to PF of WMD indicates that the types of evasion mentioned in the previous section are difficult to identify directly.

In the Spanish context, it is important to mention intermediary jurisdictions that pose threats related to PF due to the channelling of funds or the conduct of international transactions with companies exporting materials from these jurisdictions. This latter activity will be analysed within the context of the financial impact that suspicious transactions have on proliferation, with a particular focus on those that have led to investigations and potential court rulings.

[10]https://home.treasury.gov/news/press-releases/sb0082?utm_source=chatgpt.com

Table 2. National PF of WMD threats linked to the DPRK

TYPE OF THREAT	DEVELOPMENT	EVIDENCE
Designated actors	They are representatives or facilitators of activities linked to the DPRK. Intermediation in contacts or business deals that facilitate the flow of funds. Recruitment of followers.	There is no evidence of activity in Spain. There is no census of North Koreans in Spain.
Cybercrime	Channelling funds to the DPRK through cyberattacks and cyber scams. Cyberespionage.	Lazarus Group: - WannaCry 2017. An estimated 600 Spanish companies may have been affected by the attack. - Cyberespionage against a Spanish aerospace company (2021–2022).

THREAT TYPE	DEVELOPMENT	EVIDENCE
Creation of accounts in intermediary countries	Channelling of funds through the involvement of other countries.	Accounts created with Iranian interests in Switzerland, Hong Kong, Türkiye, or the United Arab Emirates.

Use of shell companies	ML with fictitious business figures. Tax evasion. Damages to the national economy.	Management of offshore accounts by currency exchange firms (in the name of shell companies that carry out sales on behalf of sanctioned entities) or Iranian professionals.
Use of front men for collections/payments	Circumvention of financial sanctions controls. Reputational damage in the case of using independent professionals. (Especially those who are regulated entities).	Direct settlements with specific bank accounts through the intermediation of professionals who coordinate the collection/payment of goods without a direct transfer to or from Iran.
Purchase of real estate by Iranians	Possibility of concealing actors who move funds for PF purposes.	In Spain, transactions have been reported, but the police units responsible for ML/TF investigations have found no evidence.

Operations linked to the proliferation of WMD involve a monetary flow that indirectly connects them to PF; this is why Law Enforcement Authorities (hereinafter, LEAs) conduct an asset investigation related to the operation.

Table 3. National proliferation threats with links to PF.

TYPE OF THREAT	DEVELOPMENT	EVIDENCE
Use of intermediary countries	Trade in dual-use goods.	Collection and payment transactions to and from Spain with companies in China, Hong Kong, and Türkiye.
Use of shell companies to divert defense materials and prohibited chemicals	Banking operations associated with the scheme and potential circumvention of customs controls.	Diverted aeronautical and dual-use materials prior to their export to Russia. Unusual volume of sales and irregular financial transfers.
Criminal organization	Operating in dual-use trade, with links to drug trafficking and human trafficking European legal entities.	A Spanish company that, between 2013 and 2018, in collaboration with another German company, illegally imported and brought into Spain night-vision and thermal imaging equipment, part of which was subsequently sold to drug trafficking organizations in Andalusia.
Exports to Iraq	Dual-use trade operation, links to ML and brokerage by high-risk third countries.	Spanish company that illegally exported radio equipment with cryptographic capabilities to Iraq.

The Statistical Information Report of the Commission for the Prevention of Money Laundering and Terrorist Financing [11]publishes data on counterproliferation investigations arising from intelligence reports submitted by SEPBLAC and on the Commission's own initiative.

Table 5. Police investigations into counterproliferation based on SEPBLAC reports

	2020	2021	2022	2023	2024
Police investigations into counter-proliferation with SEPBLAC reports	5	10	4	15	14

Source: Policía and Guardia Civil

In this table, the investigations were related to Russia, Iran, and Venezuela.

Table 6. In-house police investigations into counterproliferation

	2020	2021	2022	2023	2024
Investigations on own initiative	70	21	30	45	40
Arrested	37	3	3	8	11
Seizures (€)	3,520,882	7,000	5,405,514	1,444,263	7,430

Source: Policía and Guardia Civil

Investigations initiated on their own initiative focused on operations involving Russia, China, Pakistan, and Iran.

5.3. Emerging Threats

In the current context of growing geopolitical tension and rapid technological evolution, PF prevention mechanisms must adapt. The responses gathered from various private-sector actors reveal a highly diverse landscape, where traditional threats (sanctions evasion, use of cash, shell companies) converge with factors specific to digital and financial innovation (cryptocurrencies, cyberattacks, AI, 3D printing).

[11] https://www.tesoro.es/prevencion-del-blanqueo-y-movimiento-de-efectivo/comision-de-prevencion-del-blanqueo-de-capitales-e-infracciones-monetarias/estadisticas-e-reports/statistics

Table 7. Emerging threats identified by the private sector

THREAT TYPE	TOOLS	CHARACTERISTICS
Illicit financial channels and technological innovations	Illicit financial channels and technological innovations technological innovations Unregulated digital payment systems. Artificial Intelligence and additive manufacturing	*Exchange* hacking Alternative payment gateways and *fintech* that enable transfers to sanctioned recipients. AI, 3D printing, or biotechnology used to circumvent export controls or accelerate the production of sensitive components.
Cyberfraud	Phishing/use of *malware*	Fraud targeting crypto *wallets*
Illicit trade and logistics manipulation	Document forgery Triangulation and alternative routes	Falsified invoices and licenses to conceal the destination or beneficial owner of exported goods Use of intermediary countries allied with sanctioned regimes
Use of low-cost technologies	Illegal use of drones	In Spain, specific risks have been identified: the presence of drones in the vicinity of air bases, nuclear power plants, or prisons, but without being able to identify a clear link to PF of WMD.

6. Main Vulnerabilities

6.1. Structural vulnerabilities

6.1.1. Stemming from the regulatory framework

International sanctions adopted by the UN Security Council are not directly applicable in Spain; rather, they must first be adopted by the European Union.

Currently, Spain does not have specific criminal legislation regarding the PF of WMD. However, the European Union has adopted Directive (EU) 2024/1226 of the European Parliament and of the Council of April 24, 2024, on the definition of criminal offenses and sanctions for violations of the Union's restrictive measures. This Directive is currently in the process of being transposed into Spanish law.

6.1.2. Stemming from the implementation of UNSC sanctions

The greatest vulnerability in Spain identified in the 2014 Mutual Evaluation Report is the failure to implement UNSC sanctions "without delay." Although this obligation is met in practice due to the existence of automated procedures in the preventive systems of regulated entities, there is no such regulatory requirement, as the EU typically takes more than 24 hours to transpose UNSCR into EU law.

In 2019, Spain underwent a FATF effectiveness reassessment report, in which Immediate Outcome 11 was upgraded from moderate to significant. Among the improvements identified, despite the fact that the vulnerability mentioned in the previous paragraph continues to be detected, the capacity to identify and prosecute the evasion of financial sanctions related to PF was enhanced through investigations by LEAs and supervision by SEPBLAC.

On the other hand, the mandate of the Panel of Experts on North Korea has not been renewed, and the Panel has therefore been inactive since April 2024[12]. The dissolution of this Panel of Experts poses a significant challenge to the monitoring of sanctions

[12] https://press.un.org/en/2024/sc15648.doc.htm

violations related to the DPRK, as its reports are used to develop national security strategies and guidelines or to issue directives.

The Panel of Experts on Iran was established in 2010 by Resolution 1929 to support the 1737 Committee and monitor sanctions. Its mandate ended in 2016, with the implementation of the JCPOA and the lifting of the Security Council's sanctions regime against Iran. Following the reimposition of sanctions against Iran, UNSC Resolution 1929 (S/RES/1929 (2010) | Security Council) provided for the reactivation of this Panel if sanctions against Iran were reinstated.

6.1.3. Arising from the absence of a National Coordinating Authority on Proliferation Financing

Although Spain has not designated a single national coordinating authority on PF in accordance with FATF Recommendation 2, these responsibilities are currently being exercised by the Specialized Committee on Non-Proliferation and its working group on Financing, as well as by the Commission for the Prevention of Money Laundering and Monetary Offenses and its supporting bodies.

6.1.4. Derived from compliance by the private sector

Experience in the private sector shows that there is an increasingly clear connection between ML/FT activities; consequently, this connection also holds true for identifying transactions linked to PF. Nevertheless, identifying transactions directly linked to PF is challenging due to their inherent complexity and the sophistication of certain corporate structures that may be associated with this activity.

One of the most widespread weaknesses is the **lack of awareness and specific training** regarding the risks of PF.

6.2. Contextual or Geographical Vulnerabilities

Spain's location as a hub connecting Europe, Africa, and Latin America constitutes a commercial advantage, but it also entails exposure to the potential use of the territory as a logistics platform for illicit activities. The main vulnerabilities of Spain's geography are:

- The Strait of Gibraltar and the Algeciras customs post, a strategic hub for international trade and the covert transport of sensitive materials.
- The ports of Valencia, Barcelona, and Bilbao, due to their large capacity and high volume of traffic. This poses an operational challenge in terms of the capacity to inspect and control goods.
- Ceuta, Melilla, and the Canary Islands, due to their proximity to territories with less stringent customs controls.

In conclusion, Spain's geographic location, its logistics and port infrastructure, its regional environment, and its role in international trade increase its vulnerability. This does not necessarily imply a high risk in absolute terms, but it does require continuous vigilance, rigorous enforcement of export controls, and a strengthening of detection and analysis capabilities by competent authorities and the private sector.

6.3. Sectoral Vulnerabilities

6. 3.1. Derived from International Trade

Spain has established itself as a major international port hub[13] due to its significant international trade sector. Spain ranks fourth among European Union countries in terms of maritime cargo traffic volume, primarily through the seaport of Algeciras. The ports of Valencia and Algeciras are among the five largest European ports in terms of large container traffic[14] .

[13] Source: Statistical Yearbook of the State-Owned Port System 2023.
[14] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Maritime_transport_of_goods_at_port_level_-_quarterly_data

Generally speaking, the highest volumes are exported to Europe, followed by the United States, China, and Russia. However, despite Spain's geographical location, regions such as Africa, South America, and Oceania account for considerably lower volumes.

In terms of traded goods, general merchandise remains the predominant category by volume, accounting for 48% of the total transported. Among the main goods transported are food products, chemicals, construction materials, steel products, as well as machinery, tools, and spare parts, along with fruits, vegetables, legumes, paper, and paper pulp.

The high volume of goods may therefore pose a vulnerability when it comes to detecting the trafficking of goods and, ultimately, potential violations of international sanctions, particularly with jurisdictions that have direct relations with the DPRK and Iran.

The following table shows Spain's foreign trade data with the DPRK and Iran, including total figures and items considered to have potential dual-use[15] for the period 2020–2024[16] :

Table 8: International Trade Statistics with the DPRK and Iran

	Exports		Imports	
	Value (in thousands of €)	%	Value (thousands of €)	%
DPRK	922.44	0.0001%	10.66	0.000001%
Iran	1,079,340.68	0.06%	523,384.74	0.03%
TOTAL SPAIN	1,734,649,078.98	100%	1,930,875,347.71	100%

Source: Spain's foreign trade data https://datacomex.comercio.es/Metadata/Index

[15] The following items published in international trade statistics have been taken into account: 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 59, 72, 73, 74, 75, 76, 78, 79, 80, 81, 82, 84, 85, 86, 87, 88, 89, 90, 93.

[16] The list of items identified as potentially related to dual-use material has been provided for informational purposes only. It is important to note that the inclusion of these categories does not imply that all products falling under them are considered dual-use, but only certain specific goods, components, or substances in accordance with applicable regulations. Furthermore, the figure provided is an overestimated estimate, prepared with the aim of ensuring a margin of safety in the assessment.

Table 9: International trade statistics with the DPRK and Iran for dual-use items

	Dual-use exports		Dual-use imports	
	Value (thousands of €)	%	Value (thousands of €)	%
DPRK	425.03	0.00003%	8.15	0.000001%
Iran	850,291.17	0.06%	171,840.89	0.02%
TOTAL SPAIN	1,366,436,637.32	100%	1,078,776,052.21	100%

Source: Spain's foreign trade data https://datacomex.comercio.es/Metadata/Index

Regarding Spain's international trade relations with Iran and the DPRK, Tables 8 and 9 above show the limited significance of Spain's international trade with these two countries.

6. 3.2. Derived from Financial Sector

Although the Spanish financial sector has a solid regulatory framework and effective supervision, it faces various vulnerabilities related to PF, stemming from the complexity of financial transactions and the sophistication of networks seeking to circumvent established controls.

On the one hand, the complexity of identifying suspicious transactions is identified as a vulnerability. Furthermore, there are activities involving products such as crypto-assets and multi-stage international transfers via SWIFT, which hinder the traceability of funds.

On the other hand, correspondent banking accounts with foreign banks located in high-risk jurisdictions or with lax controls, as well as multi-stage international transfers via SWIFT, have been identified as high-risk products.

Finally, the lower level of training and awareness regarding PF constitutes an aggravating factor, creating greater difficulties than in ML/TF for identifying and reporting suspicious transactions related to proliferation.

6. 3.3. Derived from non-financial activities and professions

For this type of regulated entity, the challenges associated with implementing automated alert systems and detecting transactions linked to sanctions evasion are greater, particularly in the retail sector.

There are sectors that do not perceive the risk of PF and may be unaware of the regulations for identifying lists of designated persons and entities linked to proliferation programs, which limits their ability to act as a first line of defense.

Likewise, certain professions, particularly lawyers, notaries, or tax advisors, are more vulnerable to transactions involving shell companies or complex structures designed to conceal the beneficial owner**.** It is precisely this opacity that many proliferation networks seek to exploit to circumvent financial controls and evade international sanctions.

Another area of vulnerability lies in the trade of high-value, easily transportable goods, as is the case in the jewelry sector or among dealers in precious metals and gemstones. These goods can be used as payment instruments in international transactions without necessarily requiring the use of the traditional financial system. This characteristic makes them a potential channel for moving funds linked to the value of the goods without being detected.

6.4. Specific vulnerabilities of traded goods and services

Spain ranks ninth globally in arms exports[17] for defense materials and dual-use goods.

The year 2024 saw a notable increase in authorized values and a low implementation rate compared to other years. In summary, in 2024 a total of 5,257 export licenses were processed, of which 4,154 were approved, 111 were denied, and the rest were withdrawn, expired, or waived. The products traded are[18] :

[17] Source: World Bank. According to SIPRI (Stockholm International Peace Research Institute), Spain would be the world's ninth-largest exporter in the 2020–2024 period and eleventh in 2024.[18] Source: Ministry of Economy, Trade, and Enterprise

Defense Equipment

The total value of authorized equipment was €17.395 billion, representing an 11% increase over the previous year. A total of 2,439 licenses were issued, a 23% increase from the previous year. The total value of exports in 2024 amounted to €3.491 billion (7% less than in 2023). The "aircraft" category was the most significant in terms of value, both in authorizations and exports. Geographically, the European Union and NATO were the main destinations, accounting for 64.6% of the total. Germany and the United Kingdom were the largest recipients, focusing on aircraft, ammunition, and technology transfer. There is a growing trend in the intangible transfer of technology, software, and technical training, which consolidates Spain as a key player in European defense R&D projects.

Police and security equipment

The value of authorizations fell sharply from €4.2 million in 2023 to €1.5 million in 2024, reflecting lower demand. Despite this, actual exports rose to €2.2 million, exceeding the authorized value in 2024 due to licenses from the previous year, reaching an exceptional fulfillment rate of 147% (due to valid licenses issued the previous year).

Hunting and sporting firearms

Authorizations nearly doubled, rising from €354 million to €695 million, suggesting greater potential demand and greater efficiency in the issuance of licenses. However, actual exports remained stable at €137 million, with a realization rate of approximately 20%.

Dual-use products and technologies

Exports of dual-use goods and technologies fell by 26% compared to the previous year, reaching €293 million. On the other hand, the number of licenses granted increased by 50%, reaching 1,249, although the total authorized value decreased by 60% to €1.315 billion. The implementation rate was 22%. Furthermore, there has been an upward trend in the number of authorized licenses over the past 8 years. The main destinations by export value were Saudi Arabia (€63.6 million), France (€31.5 million), China (€39.8 million), and the United States (€16.7 million). The most exported products cover a wide range, from laboratory reagents and explosives to aerospace components and software

simulation and anti-drone systems, demonstrating an export strategy focused on various technological and industrial sectors.

Use of Drones[19]

The use of drones creates vulnerabilities in national security, with potential effects including the disruption of military operations, espionage, or the use of drones as a means to circumvent export controls and finance proliferation activities.

In summary, 2024 was characterized by a notable increase in license authorizations for Defense and Dual-Use Materials and a low overall implementation rate, although most of the licenses requested may be executed in subsequent years.

[19] 2024 Annual National Security Report

6.5. Summary of Vulnerabilities

Table 10. Vulnerabilities

Vulnerability		Variables	Consequences
Main vulnerability	**Type**		
Structural vulnerabilities	Derived from the regulatory framework Regulatory	European Regulations subject to direct transposition into Spanish law Penalties for failure to freeze funds. Lack of criminal legislation.	Reliance on European regulations can lead to delays in the adoption of international regulations at the national level; the absence of a specific criminal sanctions regime reduces the deterrent effect and makes it difficult to investigate serious sanctions violations; and the The current sanctions regime, which treats the failure to freeze funds as an administrative violation, imposes limitations on the enforcement process regarding international financial sanctions.
	Arising from the implementation of UNSC sanctions	Absence of a national regulatory framework that establishes the application "without delay."	Although this is complied with in practice due to the existence of in the preventive systems of regulated entities, it is not explicitly established as required in Immediate Outcome 11.

	Issues arising from the absence of a National Coordinating Authority	There is no authority designated by regulation.	All the powers required by the FATF methodology in this regard are being exercised by the Subdirectorate General for Inspection and Control of Capital Movements of the Public Treasury.
	Issues arising from compliance by the private sector	Difficulty in identifying transactions directly related to PF. Lower awareness of PF risks, especially in non-financial sectors that have less sophisticated monitoring systems.	Increased preventive costs for regulated entities in identifying this type of transaction. Breaches of the controls implemented by regulated entities.
Contextual or geographic vulnerabilities		Geographic location of Spain and its logistics and port infrastructure: • Strait of Gibraltar and customs at	Operational challenge regarding the capacity for inspection and control of goods and, therefore, the financial analysis involved in this operation.

		Algeciras, a strategic hub for and for the covert transport of sensitive materials. • Ports of Valencia, Barcelona, and Bilbao due to their large capacity and high volume of traffic. • Ceuta, Melilla, and the Canary Islands due to their proximity to territories with less customs control.	
Sector-Specific Vulnerabilities	Arising from International trade	Algeciras and Valencia major ports for of large containers. Algeciras ranks fourth in importance regarding the volume of goods.	Concealment of illicit goods within large volumes of imports/exports intended for the black market.

	Derived from the financial sector	Complexity in identifying suspicious transactions due to the link between ML/TF operations and PF. High-risk such as correspondent banking with Foreign located in high-risk jurisdictions or with lax controls or international transfers via SWIFT in multiple stages. Crypto operations linked to sanctions evasion.	Use of cryptoassets to move funds, especially decentralized finance platforms. Concealment of the underlying crime to evade sanctions. Operations and products that hinder transparency regarding the parties involved and the nature of the transactions.
	Derivatives of DNFBPs	Professionals acting as intermediaries for shareholding structures or who are involved in transactions relatedcorporate actions, especially	Difficulty in identifying the beneficial owner. Use of professionals as tools to evade sanctions.

		when the party involved is not incorporated in Spain or is part of a complex structure. Trade in high-value, easily transportable goods used as payment in international trade transactions.	Ease of moving funds when luxury goods are used.
Product-specific vulnerabilities and services traded		The vulnerable commercial products are: defense equipment, police equipment and security equipment, hunting and sporting weapons, and technologies considered dual-use, and the use of drones.	Given the volumes traded, may conceal threats linked to law enforcement. The use of drones creates vulnerabilities in national security in addition to having an economic impact linked to PF.

7. Risks

7.1. Inherent risks

The analysis of threats and vulnerabilities, combined with the limited evidence related to PF, results in a **medium-to-low inherent risk** rating **for PF in Spain.**

A risk matrix has been developed to identify which regulated entities are subject to a higher risk of financial fraud.

Article 10(3) of Regulation (EU) 2024/1624 of the European Parliament and of the Council of May 31, 2024, provides that *"With the exception of credit institutions, financial institutions, crowdfunding service providers, and crowdfunding intermediaries, supervisors may decide that documented risk assessments of the entire business activity of each obligated entity are not required if the specific risks inherent to the sector are clear and have been understood."*

The inherent risk by sector is shown in the following table:

Table 11. Sector-specific inherent risk

Letter	Obligated Entity	Inherent Risk
a	Credit institutions	
b	Life insurance/investment entities and insurance brokers	
c	Investment firms	
d	Management companies of Collective Investment Institutions and investment companies without a management company	
e	Pension fund management entities	
f	Venture capital management companies and venture capital companies without a management company	
g	Mutual guarantee companies	
h	Electronic money institutions and payment institutions	
i	Persons engaged professionally in currency exchange activities	
j	Postal services engaged in money order or transfer activities	
k	Intermediaries in the granting of loans or credit	
l	Real estate developers and agents in sales/leases ≥€120,000/€10,000 per month	
m	Auditors, external accountants, tax advisors, and those who provide tax	
n	Notaries and registrars	
ñ	Attorneys, solicitors, and professionals in financial/real estate	
o	Third-party service providers	
p	Gambling casinos	
q	Professional trade in jewelry, precious stones, or precious metals	
r	Professional trade in art/antiques and intermediaries, including free ports	
s	Activities under Law 43/2007 (goods with a price refund offer)	
t	Professional deposit, custody, or transport of funds or means of payment	
u	Management, operation, and marketing of lotteries and games of chance	
and	Payment and clearing/settlement system operators, card	
z	Providers of virtual-to-fiat currency exchange and digital wallet custody wallets	
-	Other cryptoasset service providers	

Key

High	High/ Substantial	Substantial	Substantial/ Medium	Medium	Medium/ Low	Low

7.2. Mitigation measures

7.2.1. Institutional Mitigation Measures

In the case of the EU, policy toward the DPRK is guided by the principle of *critical engagement*, which combines multilateral and autonomous sanctions with a willingness to engage in dialogue, always with the goal of verifiable denuclearization and the preservation of the international non-proliferation regime. Spain aligns with this approach, limiting itself to compliance with the sanctions and control framework established by the EU.

With regard to Iran, EU controls have been strengthened following the "snapback" of sanctions in 2025, which resulted in the amendment of Regulation (EU) No. 267/2012. This entails the reintroduction of financial restrictions, the freezing of funds, and a ban on transfers to designated entities, along with strengthened oversight and transparency mechanisms. Spain implements and enforces these provisions, ensuring the effective freezing of funds and the blocking of transfers of sensitive technology, which constitutes the primary regulatory mitigation measure currently in place against Iranian PF.

Regarding potential cooperation agreements, the EU maintains a limited framework for dialogue with both the DPRK and Iran, but always subject to strict safeguards. In the case of North Korea, there are no bilateral cooperation projects with Spain, and trade is virtually non-existent due to sanctions and restrictions. In the case of Iran, diplomatic channels remain open in the EU and in Spain, albeit with a very limited scope. Cooperation is limited to diplomatic exchanges.

At the national level, Spain has specialized units under the National Security Directorate, as discussed in Section 4.

With specific regard to proliferation financing, the Treasury, in its capacity as regulator, publishes various documents concerning the applicability of the sanctions set forth in UNSC resolutions[20], and is also responsible for authorizing transfers of funds subject to countermeasures. Finally, SEPBLAC combines its financial intelligence analysis and supervisory functions with a risk-based approach, enabling it to identify vulnerabilities and supervise regulated entities.

[20] https://www.tesoro.es/prevencion-del-blanqueo-y-movimiento-de-efectivo/sanciones-financieras

In the case of trade in defense equipment, other equipment, and dual-use products and technologies, the export of these products without the corresponding license constitutes a violation of the law under the provisions of the Criminal Code and Organic Law 12/1995 of December 12 on the Suppression of Smuggling.

7.2.1.1. JIMDDU: Interministerial Regulatory Board for Foreign Trade in Defense and Dual-Use Materials.

Spain's export control regime is overseen by the JIMDDU, which is responsible for registering all companies that manufacture or trade in defense equipment and other equipment, as well as for approving any transactions related to the export of these products from Spain.

The JIMDDU reviews each export license application and authorizes only those transactions in which there is no risk that the exported products will be diverted for military use or for the manufacture of WMD.

The JIMDDU examines the Spanish exporting company, the exported product, and the recipient and end-user of the product.

In addition, Spain participates in multilateral export control agreements. Policía Nacional and Guardia Civil, which are responsible for investigating possible violations of export controls, are both part of the JIMDDU. The SEPBLAC participates in the meetings of the working group that prepares for JIMDDU meetings, collaborating in the exchange of intelligence information.

7.2.1.2. Special Registry of Foreign Trade Operators (Registro Especial de Operadores de Comercio Exterior, REOCE)

Its purpose is to collect and record information on operators engaged in foreign trade of defense equipment, hunting and sporting weapons, police and riot control equipment, as well as dual-use products and technology. These activities are subject to control and regulation under Royal Decree 679/2014, of August 1.

7.2.1.3. *Integrated Electronic Warfare System Against UAS and SUCCAUL Program*[21]

As a result of the growing threat posed by the illicit use of drones, Spain has strengthened its capabilities with specific detection and neutralization systems, such as the Comprehensive Electronic Warfare System Against UAS (SIGLO-CD) and the SUCCAUL program, aimed at the surveillance, identification, and neutralization of unmanned aerial vehicles in sensitive areas.

Part of this strategy involves identifying the financial networks that facilitate the acquisition of these platforms through front companies, triangulated transactions, or covert payments.

7.2.2. Commercial mitigation measures

While there are trade vulnerabilities linked to Spain's significant export volume, the existing regulatory framework allows for the inspection of goods in certain cases, which mitigates the risk:

- For agri-food or phytosanitary products, health certification is required.
- Defense-related material, other dual-use materials, products, and technologies are subject to export licensing requirements. The legal framework governing the trade of dual-use goods is extensive in Spain and is included in Annex 2.
- Dangerous or restricted goods, meanwhile, require document verification.
- In cases where goods originate from countries subject to sanctions or trade restrictions, special monitoring is applied.

[21] National Security Report 2024

- Finally, whenever there is suspicion of fraud, smuggling, or tax evasion, Customs has the authority to conduct random inspections based on its specific regulations[22] .

In addition, the Department of Customs and Special Taxes of AEAT, applies an export control procedure in Spain, pursuant to Article 46 of the Union Customs Code—Regulation (EU) No. 952/2013—based on risk analysis. Under this regulatory framework, it is possible to establish exceptions through certification and simplified procedures, which exempt certain exporters from routine inspections.

These general procedures are supplemented by additional controls for goods characterized by their dangerous nature and their connection to sanctions regimes, which limits the possibility of violating international sanctions through the Spanish customs system.

7.2.3. Beneficial ownership control to prevent the provision of assets to sanctioned persons [23]

Spain is not a global hub for corporate formation where there have been cases in which the beneficial owners of legal entities could be linked to the evasion of sanctions or the creation of companies.

Furthermore, notaries in Spain have developed a system for detecting complex legal transactions and structures following the establishment of the Centralized Prevention Body, Órgano Centralizado de Prevención (hereinafter, OCP) within the General Council of Notaries, which utilizes tools such as the Single Computerized Notarial Index—which cross-references information from millions of notarized transactions nationwide, all of which are thoroughly analysed by the OCP's specialized team— or the Beneficial Ownership Database, which allows notaries, authorities, and regulated entities to verify the accuracy of declarations by the ultimate beneficial owners of legal entities conducting transactions subject to public deeds.

[22] Organic Law 12/1995, of December 12, on the Suppression of Smuggling; Law 58/2003, of December 17, the General Tax Law (LGT); and Royal Decree 335/2010, of March 19, regulating the control of customs surveillance services.

[23] Source: Addendum to the National Risk Analysis, 2024

As an additional measure, and within the European framework, in 2021, Royal Decree-Law 7 of 2021, dated April 27, introduced the Third Additional Provision of Law 10/2010, dated April 28, for the creation of a Central Register of Beneficial Ownership, Registro Central de Titularidades Reales (hereinafter, RCTIR)

In addition, Spain is part of the European BORIS project, which consists of the interconnection of central registers of beneficial owners within the European Union.

7.2.4. Measures implemented by the financial sector.

Financial institutions have developed a comprehensive framework of policies and procedures aimed at preventing and detecting transactions linked to the proliferation of WMD. The measures implemented are outlined below.

- Risk-based customer management approach: all customers are subject to due diligence measures, and "high-risk" customers are subject to an enhanced procedure.
- Use of algorithms capable of detecting partial matches and potential pseudonyms that identify, in real time, matches with lists provided by the UNSC and the EU, among others.
- Limits on cash deposits in accordance with the provisions of Law 10/2010 of April 28.
- Request for relevant supporting documentation in the event of unusual transactions or those inconsistent with the customer's activity.
- Automated transaction monitoring systems operating 24 hours a day.
- Improvement of specific cybersecurity measures: intrusion detection, protection of the banking system, and collaborative monitoring among the fraud, cybersecurity, and anti-money laundering units, with the aim of identifying and blocking funds derived from malicious online activities.
- Internal audits and collaboration with public and private entities to continuously adapt procedures to new threats and trends.

Regulation (EU) 2024/1624 of the European Parliament and of the Council of May 31, 2024, requires specific measures to address the risk of PF and sanctions evasion.

7.3. Residual risk

Taking into account existing mitigation measures, their degree of implementation, and their proven effectiveness in key sectors, it is concluded that **Spain's residual risk regarding PF for all sectors is reduced to low.**

In accordance with Article 10.3 of Regulation (EU) 2024/1624 of the European Parliament and of the Council of May 31, 2024, and based on the analysis conducted, non-financial obligated entities under Law 10/2010 of April 28 with a residual risk of below average or high would not be required to conduct a self-assessment analysis of PF, based on the risk rating obtained.

The residual risk for each sector after applying the mitigating measures can be seen in the following table:

Table 11. Sectoral residual risk

Letter	Regulated Entity	Residual Risk
to	Credit institutions	
b	Life insurance/investment companies and insurance brokers	
c	Investment firms	
d	Management companies of Collective Investment Institutions and investment companies without a management company	
e	Pension fund management entities	
f	Venture capital management companies and venture capital companies without a management company	
g	Mutual guarantee companies	
h	Electronic money institutions and payment institutions	
i	Individuals who engage in currency exchange on a professional basis	
j	Postal services involved in money orders or transfers	
k	Intermediaries in the granting of loans or credit and related activities	
l	Real estate developers and agents in sales/leases ≥€120,000/€10,000 per month	
m	Auditors, external accountants, tax advisors, and those providing tax assistance	
n	Notaries and registrars	
ñ	Attorneys, solicitors, and professionals in financial/real estate transactions	
o	Third-party service providers	
p	Casinos	
q	Professional trade in jewelry, precious stones, or precious metals	
r	Professional art and antique dealers and brokers, including private dealers free ports	
s	Activities under Law 43/2007 (goods with a price refund offer)	
t	Professional deposit, custody, or transport of funds or means of payment	
u	Management/operation/marketing of lotteries and games of chance	
y	Payment and clearing/settlement system operators, card operators	
z	Providers of virtual-to-fiat currency exchange and wallet custody	
-	Other cryptoasset service providers	

High	High/Substantial	Substantial	Substantial/Medium	Medium	Medium/Low	Low

APPENDIX 1—Export Control Statistics[24]

Year	Destination	Content	Value (€)	Reason
2024	United United Arab	3 Autopilot systems, software units for UAVs, and laboratory reagents for in vitro diagnostics		Risk of diversion to a country subject to EU sanctions and the existence of denials
2024	India	2 Autopilot vectors		Risk of diversion to a country subject to EU sanctions and existence of denials
2024	Kazakhstan	1 Variable Frequency Drives (VFD)		Risk of diversion to a country subject to EU sanctions and existence of denials
2024	Nigeria	1 Unmanned Aerial Vehicles (UAVs) and their components		Risk of diversion to a country subject to EU sanctions and existence of denials
2024	People's Republic of China	1 Drilling machine		Risk of diversion to a country subject to EU sanctions and the existence of denials

[24] Spanish statistics on exports of defense equipment, other equipment, and dual-use products and technologies. Ministry of Home Affairs, Economy, Trade, and Enterprise https://comercio.gob.es/ImportacionExportacion/Informes_Estadisticas/Paginas/Hitorico_Material_Defensa.aspx

2024	Russia	3 Automatic analyzer and high-pressure food processing equipment		EU Sanctions
2024	Cuba	7 Cartridges of various calibers, hunting shotguns of various calibers, and hunting rifles of various calibers		Article 8.d) of Law 53/2007. Restrictions arising from international law (Embargo)
2024	Guinea-Bissau	One 12-gauge shotgun cartridge, non-metallic ammunition.		Internal situation and risk of use in internal repression
2024	Venezuela	Perazzi 12-gauge shotgun		Article 8.d) of Law 53/2007. Restrictions under International Law (Embargo)
2023	Serbia	12 tons of trinitrotoluene	160,000	Extension of products in the REOCE denied
2023	Bangladesh	5.5 million 12-gauge rubber-ball hunting cartridges	2,700,000	Criteria 2 and 3[25] of Common Position 2008/944/CFSP

[25] Criterion 2: Respect for human rights in the country of final destination
A Member State must deny an arms export if there is a clear risk that the equipment could be used:

- For internal repression (e.g., suppression of peaceful demonstrations, torture, or human rights violations).
- To facilitate serious violations of international humanitarian law.

Criterion 3: A Member State must deny an export if the equipment contributes to:

- The escalation of internal tensions or armed conflicts.
- Internal instability that could lead to civil wars, coups d'état, or ethnic or religious violence.

2023	Guinea-Bissau	2.9 million 12-gauge hunting cartridges	1,700,000	Criteria 4[26] and 7[27] of the Common Position 2008/944/CFSP
2023	India	Autopilots and control software for UAVs	1,300,000	Risk of diversion to a country sanctioned by the EU
2023	China	Software logic equipment for data simulation, uncooled cameras, nickel-based metal powder	444,473	Risk of technology transfer for military use
2023	Russia	Reagents, automated analyzers, blood test strips, freeze dryer	417,873	Imposition of EU sanctions on Russia
2022	Pakistan	670 sporting pistols with magazines	175,175	Lack of information on the recipient and risk of diversion to a sanctioned country

[26] Criterion 4: Maintenance of regional peace, security, and stability
Member States shall deny an export license where there is a clear risk that the intended recipient may use the military technology or equipment proposed for export to attack another country or to enforce a territorial claim by force. In assessing such risks, Member States shall take into account, among other things:

a) the existence or likelihood of an armed conflict between the recipient country and another country;
b) a territorial claim by a neighboring country that the recipient has attempted to enforce or has threatened to obtain by force in the past;
c) the likelihood that the military technology or equipment will be used for purposes other than the recipient's national security and legitimate self-defense;
d) the need to avoid significantly undermining regional stability.

[27] Criterion 7: Risk of diversion of the exported equipment
A Member State must deny an export if there is a clear risk that:

- The exported equipment could be re-exported without authorization to another country or unauthorized group.
- The export could fall into the hands of terrorist or criminal groups.
- There are insufficient guarantees regarding the control of the material in the destination country.

2022	Burkina Faso	5.5 million hunting cartridges	1,600,000	Criterion 7 of Common Position 2008/944/CFSP
2022	Guinea-Bissau	13.5 million hunting cartridges	5,400,000	Criteria 4 and 7 of Common Position 2008/944/CFSP
2022	Cuba	2,500 tear gas and smoke canisters, 40 light, sound, and tear gas devices	350,000	Criterion 2 of Common Position 2008/944/CFSP
2022	Central African Republic	50,000 tear gas cartridges	2,100,000	Criterion 2 of Common Position 2008/944/CFSP
2022	China	9 uncooled infrared cameras, 2 scanning cameras, 1 power control system	77,000	Risk of diversion to a proliferation program
2022	Russia	153 stainless steel and aluminium bronze globe valves, 26 gate valves, and replacement parts	1,400,000	EU sanctions and risk of diversion to the military industry
2022	Israel	418 and inertial navigation systems for UAVs, 2 evaluation boards, 18 autopilot vectors	700,000	Risk of deviation in use and destination

2022	Türkiye	1 machining center	115,000	Risk of diversion to a sanctioned country
2022	Egypt	5 autopilot UAV carriers	40,344	Risk of diversion due to lack of information on the recipient
2021	Burkina Faso	11.4 million hunting cartridges	1,200,000	Criterion 7 of Common Position 2008/944/CFSP
2021	China	996 converters, simulation software, 200 kg of nickel-based powder	343,252	Risk of diversion for military use and denials by other countries
2021	Russia	1 frequency module, 2 uncooled cameras	288,424	EU sanctions and risk of diversion to military use
2020	Ukraine	1 machining center	846,597	Risk of diversion to the manufacture of military equipment for re-export to a sanctioned third country
2020	China	30 imaging sensors	128,250	Risk of diversion to military use and existence of export controls by other countries

ANNEX 2. Legal framework governing the trade in dual-use goods.

- Law 53/2007, of December 28, on the control of foreign trade in defense and dual-use items.

- Royal Decree 679/2014, of August 1, approving the Regulations on the control of foreign trade in defense equipment, other equipment, and dual-use products and technologies.

- Royal Decree 494/2020, of April 28, amending Royal Decree 679/2014, of August 1, approving the Regulations on the control of foreign trade in defense equipment, other equipment, and dual-use products and technologies.

- Royal Decree 414/2022, of May 31, amending the Regulations on the Control of Foreign Trade in Defense Material, Other Material, and Dual-Use Products and Technologies, approved by Royal Decree 679/2014, of August 1.

- Order ECM/551/2025, of May 30, amending Annexes I.1, III.1, III.3, III.4, and III.5 of the Regulations on the Control of Foreign Trade in Defense Material, Other Material, and Dual-Use Products and Technologies, approved by Royal Decree 679/2014, of August 1.[28]

- Council Regulation (EU) 2021/821 of May 20 establishing a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items, as updated by Commission Delegated Regulation (EU) No. 2022/1 of October 20.

[28] Pursuant to Spain's commitments in various international forums combating proliferation, collaboration with EU Member States, and national security requirements, an annual update is published listing the products subject to export controls. The most recent update is cited. An update will be required in 2026 in accordance with the new
.

ACRONYMS

AEAT	Agencia Estatal de Administración Tributaria (Spanish Tax Administration Agency)
AEB	Asociación de Banca Española (Spanish Banking Association)
AML/CFT	Anti-Money Laundering and Counter-Terrorist Financing
CASP	Crypto-Asset Service Providers
CGPJ	Consejo General del Poder Judicial (General Council of the Judiciary)
CITCO	Centro de Inteligencia contra el Terrorrismo y el Crimen Organizado (Centre for Intelligence against Terrorism and Organised Crime)
CNI	Centro Nacional de Inteligencia (National Intelligence Centre)
DNFBPs	Designated non-financial businesses and professions
DPRK	Democratic People's Republic of Korea
EU	European Union
FATF	Financial Action Task Force
JCPOA	Joint Comprehensive Plan of Action
JIMDDU	Junta Interministerial Reguladora del Comercio Exterior de Material de Defensa y de Doble Uso (Interministerial Regulatory Board for Foreign Trade in Defense and Dual-Use Materials)
LEA	Law Enforcement Agencies
ML	Money Laundering
OCP	Órgano Centralizado de Prevención (Centralised Prevention Agency)
PF	Proliferation Financing
RCTIR	Registro Central de Titularidades Reales (Central Register of Beneficial Ownership)
REOCE	Registro Especial de Operadores de Comercio Exterior (Special Register of Foreign Trade Operators)
SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones (Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences)
TF	Terrorist Financing
UN	United Nations
UNACC	Unión Nacional de Cooperativas de Crédito (National Union of Credit

	Cooperatives)
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolutions
WMD	Weapons of Mass Destruction