ADVISORY NOTE

SANCTIONS & PROLIFERATION FINANCING

DATE: 25 August 2025

This **ADVISORY NOTE** is produced by the Australian Sanctions Office (ASO), in the Department of Foreign Affairs and Trade, for use by Australian government agencies, individuals, businesses or other organisations whose activities are subject to Australian sanctions laws (regulated entities). This advisory note outlines the sanctions obligations and best practises for identifying, assessing and mitigating proliferation financing risk. This advisory note supports regulated entities in strengthening their compliance frameworks and compliance with national laws and international standards.

Term	Definition
Consolidated List	See **Designated person or entity**.
Designated person or entity	A person or entity listed under Australian sanctions laws. Designated persons and entities are subject to targeted financial sanctions. Listed persons may also be subject to travel bans. See DFAT website for further information. Some sanctions legislation also refers to these persons and entities as 'proscribed persons and entities'. DFAT keeps a Consolidated List of designated persons and entities, available on the Department's website.
Dual use	Goods, technology or equipment designed or suitable for both civilian and military purposes
FATF	The Financial Action Task Force is the global money laundering and terrorist financing standard setter. The FATF's international standards aim to prevent money laundering and terrorist financing and the harm they cause.
Proliferation Financing	The act of providing funds or financial services for the manufacture, acquisition, possession, development, or transport of nuclear, radiological, chemical, or biological weapons and their means of delivery, in violation of national or international laws.
Reasonable precautions and due diligence	Reasonable precautions and due diligence are not defined terms but generally refer to the steps and measures a regulated entity must take to ensure it does not engage in sanctioned activities. This includes implementing robust internal controls, screening transactions and parties against the Consolidated List. It also requires that staff are adequately trained to recognise and respond to potential sanctions risks. This is a relative standard given what constitutes 'reasonable' can vary based on a range of factors. These include the size and nature of a business, the complexity of transactions, affected geographic areas, and the specific sanctions regulations in place. Consequently, what is deemed sufficient for one entity may not be for another, making the concept inherently flexible and context dependent.
Regulated entity	A government agency, individual, business or other organisation whose activities are subject to Australian sanctions laws.

Sanctions permit	A sanctions permit is authorisation from the Minister for Foreign Affairs (or the Minister's delegate) to undertake an activity that would otherwise be prohibited by an Australian sanctions law. All permits issued under autonomous sanctions frameworks must meet the same criteria, in particular that the Minister must not grant the permit unless the Minister is satisfied that granting the permit is in the 'national interest'.
Sanctioned vessels	A vessel that: • has been designated, or included in a class of vessels, that has been designated as a sanctioned vessel by the Minister under the *Autonomous Sanctions Regulations 2011*; • has been designated by the Committee of the Security Council established under paragraph 12 of the UNSC Resolution 1718 (2006); • has been specified by the Minister under the *Charter of the United Nations (Sanctions – Democratic People's Republic of Korea) Regulations 2008 (DPRK Regulations);* or • is a DPRK vessel, including DPRK flagged or registered vessel.

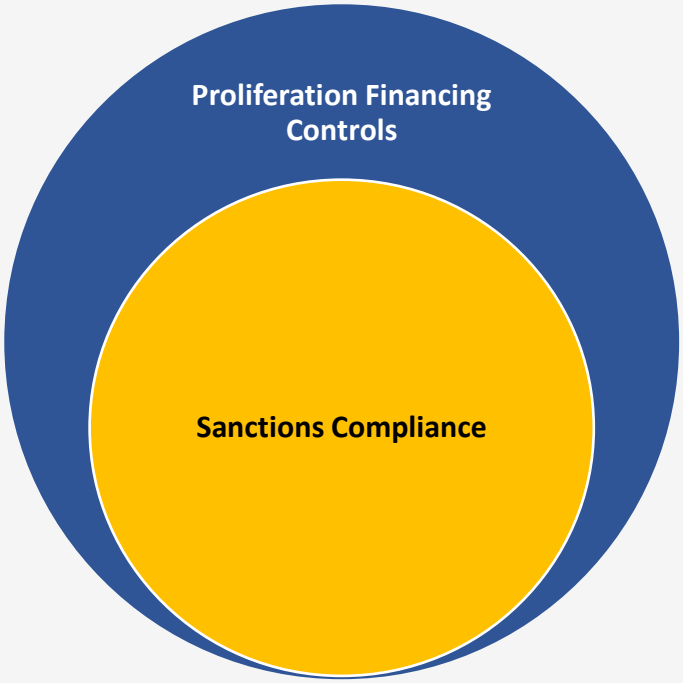
ADDRESSING SANCTIONS AND PROLIFERATION FINANCING RISKS

A strong sanctions compliance framework is an essential part of proliferation financing controls for the financial sector. Readers are recommended to refer to the sanctions compliance toolkit and self-assessment tool. When assessing your business or services for proliferation financing risks, particular consideration should be directed to:

- Customer risk factors (e.g.: links to sanctioned country/ies, sector)
- Product/service risk (e.g.: trade finance, correspondent banking)
- Geographic risk (e.g.: high-risk jurisdictions, sanctioned countries)
- Transaction patterns (e.g.: complex routing, dual-use goods).

Activities, such as sanctions screening, risk assessments and customer due diligence can further mitigate proliferation financing risks. Effective sanctions compliance and proliferation financing risk management are critical to upholding the integrity of the financial system and contributing to international peace and security. Institutions should implement a proportionate, risk-based framework and be alert to evolving threats.

The regulated community should be aware that sanctions compliance and anti-money laundering and counter terrorism financing (AML/CTF) controls alone may be insufficient for all businesses to address proliferation financing risks. There are some specific proliferation financing indicators that sit outside sanctions controls. Further information and resources on potential indicators are listed at the end of this advisory.



Legal and Regulatory Framework

Proliferation financing is governed by a number of international and domestic obligations. Entities should be familiar with:

- *The Charter of the United Nations Act 1945*, and relevant United Nations Security Council Resolutions (UNSCRs)
- Australian Sanctions Regulations and Rules
- Relevant FATF Recommendations (e.g. Recommendation 7 - Targeted financial sanctions related to proliferation)
- Defence Export Controls

United Nations requirements:

- UNSCR 1540 (2004) requires all states to: adopt and enforce appropriate effective laws which prohibit any non-state actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them.

- UNSCR 2325 (2016) requires greater attention upon: enforcement measures; measures relating to biological, chemical, nuclear weapons; proliferation finance measures; accounting for and securing related materials; and national export and transhipment controls.

FATF requirements:

- FATF Recommendation 7 (Targeted financial sanctions related to proliferation) requires countries to implement targeted financial sanctions to comply with UNSCRs relating to the prevention, suppression and disruption of proliferation of weapons of mass destructions (WMD) and its financing.

- **Call to action on DPRK and Iran,** FATF also calls upon countries to apply counter-measures to protect the international financial system from, amongst other things, the proliferation financing risks emanating from certain high-risk jurisdictions, and under FATF Recommendation 19, countries are expected to respond – as of 13 June 2025 there are specific calls to action to address the proliferation financing threats posed by DPRK and Iran.

AML/CTF Requirements

- **AML/CTF Act:** As of 31 March 2026, businesses regulated under the AML/CTF Act will be required to identify and assess their proliferation financing risks and develop and maintain policies to manage and mitigate these risks. These businesses are also required to apply enhanced customer due diligence in relation to customers in high-risk jurisdictions identified by the FATF, including DPRK and Iran. Regulated businesses will also be required to collect and verify information to establish whether their customer and certain associated persons are designated for targeted financial sanctions.

Countries of proliferation concern

Several countries are the subject of Australian sanctions, including UNSC sanctions, due to the situation of international concern about the ambition of some countries to develop or acquire weapons of mass destruction, including nuclear, radiological, chemical, and biological weapons. Iran and the DPRK are two countries of specific concern. See DFAT website, Sanctions Frameworks for more information.

Iran requirements:

Australia imposes sanctions against Iran under both UNSC and autonomous sanctions frameworks. For more information, please refer to the DFAT sanctions website and relevant legislation.

- **UNSCR 2231 (2015)** restricts the export of certain goods, commercial activities and the provision of assets.
- **Australian autonomous sanctions** restricts the export for certain goods, certain services, providing assets to designed persons or entities, dealing with assets of designated persons and entities, and travel bans on designated persons.
- **FATF call to action**[1] on Iran calls for countries to apply effective counter-measures, in line with FATF Recommendation 19.

Democratic People's Republic of Korea

DPRK entities and individuals are listed under both UNSC and Australian autonomous sanctions, as well as sanctions on particular goods and services. For more information, please refer to the DFAT sanctions website and relevant legislation.

- **UNSC 2270 (2016)** - includes activity-based and category-based targeted financial sanctions. Requirement to prevent financial transactions related to DPRK WMD program. A requirement to prevent opening and operation of branches and subsidiaries of DPRK banks. There is also a requirement to freeze assets/economic resources (including vessels).
- **UNSC 2371 (2017)** - includes prohibitions on new or expanded joint ventures and cooperative commercial entities with the DPRK.

[1] High-Risk Jurisdictions subject to a Call for Action - 13 June 2025

- UNSCR 2375 (2017) - includes prohibitions on all joint ventures or cooperative entities or expanding existing joint ventures which involve entities or individuals

- Australian autonomous sanctions include restrictions on certain commercial and other activities, restrictions on providing assets to designated persons or entities, restrictions on dealing with the assets of designated persons or entities, travel bans on designated person, and particular powers in respect to DPRK vessels.
- FATF call to action against DPRK[2] requires all countries to apply the following counter-measures to protect their financial systems from the money laundering, terrorist financing, and proliferation financing threat emanating from the DPRK:
    - terminate correspondent relationships with DPRK banks;
    - close any subsidiaries or branches of DPRK banks in their countries; and
    - limit business relationships & financial transactions with DPRK persons.

Defence Export Controls

Defence Export Controls (DEC)[3] is the Commonwealth regulator for the responsible movement of Defence-related goods, technology and services both within and outside Australia. DEC supports stakeholders from government, industry, higher education and research sectors, and private individuals to meet their obligations under Australia's export control laws. This involves:

- enabling use of the Australia, United Kingdom and United States licence-free environment
- assessing applications to export, supply, publish, or broker military and dual-use goods and technology listed on the Defence and Strategic Goods List
- issuing permits or licences (including for brokers) for such transfers if they are determined to not prejudice Australia's defence, security or international relationships
- prohibiting the export, supply or provision of goods, technology or services that may be used for, or to assist, a Weapons of Mass Destruction program.

Through its operations, DEC plays a fundamental role in ensuring Australia upholds its international obligations through participation in a series of multilateral non-proliferation and export control regimes.

METHODOLOGIES, HIGH RISK SECTORS, RED FLAGS & INDICATORS

Sectors that are high risk for proliferation financing exploitation

In the recent FATF proliferation financing risk assessment and methodology report, the following sectors were noted as being at a higher risk of exploitation by entities of individuals attempting to move funds for the purpose of proliferation.

[2] High-Risk Jurisdictions subject to a Call for Action - 13 June 2025
[3] Export controls framework | Defence

Trust and company service providers: creating corporate entities that proliferators use to obscure the links between a financial transaction and a designated person or entity. In Australia this may include law firms, accounting firms, corporate service providers, and financial planners and self-managed super funds.

Dealers in precious metals and stones: providing an alternative method for proliferators to surreptitiously move financial resources across international borders.

Virtual Asset Service Providers (VASPs): provide products to proliferators and a platform for moving sums of money across international borders instantly. VASPs includes digital currency exchanges (DCEs), and some fintech and decentralized financial (DeFi) sector. The ASO has produced specific guidance to the DCE and Fintech and DeFi sectors, available on the DFAT website Guidance notes.

The maritime sector: proliferators also exploit the maritime sector, which provides a method to deliver components and materials for use in WMD, or their delivery systems, and to engage in illicit revenue raising activities to finance WMD programmes in violation of UNSCR provisions. The ASO has produced specific guidance to the maritime sector available at the DFAT website.

Academic and research partnerships: Australian universities and research bodies may be targeted for knowledge transfer or intellectual property theft. Foreign researchers or students embedded in collaborative projects transfer information or technology back to high-risk jurisdictions. The ASO has produced specific guidance to the university sector which is available on the DFAT website.

Known proliferation financing methodologies targeting Australia and the region

In Australia the following methodologies have been identified targeting Australia:

DPRK Fraud: the DPRK is reportedly raising revenue for its WMD programme through fraudulent activities. This includes the use of DPRK IT workers (see advisory note), cyber-attacks, fake business ventures and romance scams.

The use of Front or Shell Companies: including establishing or using pre-existing companies to conduct trade or move funds that support proliferation activities. These companies often have limited or no physical or online presence.

Misuse of Dual-Use Goods: including purchasing dual-use goods from Australian businesses, often presenting as a legitimate overseas company. Australian companies have previously been asked to send goods to a freight forwarder in a transshipment hub. This methodology will often involve unusual shipping routes or resistance to producing end user certificates.

Trade-Based Money Laundering (TBML): TBML techniques have been identified as a common methodology to disguise proliferation financing. This may include manipulating trade invoices, false documentation and end user certificates.

Use of Professional Intermediaries: including using trust and company services providers who can be unknowingly used to provide services for proliferation finance. This will often involve clients who provide incomplete or inconsistent information.

Misuse of the Financial Sector, including cryptocurrencies and Fintech Platforms: The Australian financial system can be unknowingly used to obfuscate proliferation financing. This can include layering through correspondent accounts and funneling payments into cryptocurrency or alternative remittance systems.

Potential red flags or indicators

Transactions or trade relating to WMD proliferation often have overlapping indicators with trade-based money laundering. The list below contains potential red flags or indicators for proliferation financing and sanctions evasion. This should not be treated as an exhaustive list.

- Parties located in countries of proliferation or sanctions concern or have known links to these countries (e.g.: DPRK and Iran).
- Parties have similar or overlapping details (such as address or employment with entities or individuals who are sanctioned).
- Parties conduct business in goods/technical controlled goods.
- Parties involved in business or transactions are inconsistent with their public or business profiles.
- The ultimate beneficiary or end user is not identified.
- The goods being traded are labelled with incorrect Australian Harmonized Export Commodity Classification (AHECC) code, exports classifications or description.
- Unusual shipping routes or transshipment points.
- Use of front or shell companies, including obscured ownership structures or lack of transparency.
- Trade in dual-use goods without clear end-use or end-user.

DUE DILIGENCE

Potential countermeasures and due diligence measures for high-risk customers or transactions

Below is a list of potential due diligence measures that should be applied to address sanctions or proliferation financing risks:

- Integrate proliferation financing risks into broader sanctions and AML/CTF compliance frameworks
    - screen and monitor customers against the consolidated list
    - train staff on proliferation financing indicators and how to escalate matters.
- Conduct enhanced due diligence upon the identification of high-risk customers or transactions, including seeking further information on:
    - ultimate beneficial ownership (UBO) on companies and trusts
    - sources and destinations of funds
    - end-use of goods and services
    - parties to trade transactions
- Financial institutions must consider their AML/CTF obligations. Businesses regulated under the AML/CTF Act must also consider their AML/CTF obligations, including:

- identify and assess the proliferation financing risk the business reasonably faces during the provision of regulated services
- develop, maintain and comply with AML/CTF policies to manage and mitigate proliferation financing risk, and ensure the business does not contravene targeted financial sanctions
- collect and verify information to establish whether a customer (or certain associated persons) is designated for targeted financial sanctions
- consider sanctions compliance as part of entering into correspondent banking relationships and nested services relationships
- submit a suspicious matter report if the business suspects it holds information relevant to the investigation or prosecution of an Australian sanctions offence.

Further information and resources

While this advisory note provides a framework for understanding key sanctions risks and compliance requirements, it does not cover every possible scenario. Sanctions compliance is a dynamic, ongoing process rather than a one-time assessment. Sanctions measures and associated risks are constantly evolving and require regulated entities to continuously monitor and reassess their compliance strategies. Regulated entities are encouraged to seek independent legal advice on their specific situation and to ensure thorough due diligence in all activities.

Further information is available on the DFAT website or by making an enquiry to sanctions@dfat.gov.au.

Other useful resources

AUSTRAC: Proliferation Financing in Australia - National Risk Assessment

DEC: Export controls framework | Defence

FATF: Guidance on Proliferation Financing Risk Assessment and Mitigation

RUSI: Guide to Conducting a National Proliferation Financing Risk Assessment: 2024 | Royal United Services Institute