**ADMINISTRATION FOR THE PREVENTION OF MONEY LAUNDERING**

**August 2024**



**WEAPONS OF MASS DESCTRUCTION PROLIFERATION FINANCING**

**TYPOLOGIES**

Contents

[INTRODUCTION 2](#_Toc188947100)

[COMPARISON OF CHARACTERISTICS – MONEY LAUNDERING, TERRORISM FINANCING, PROLIFERATION FINANCING 3](#_Toc188947101)

[INDICATORS OF WMDPF, TABLE SHOWING HOW (FATF) INDICATORS WERE APPLIED IN CASES FROM INTERNATIONAL PRACTICE 4](#_Toc188947102)

[TYPOLOGIES – DESCRIPTION, ILLUSTRATIONS, TRIGGERS FOR IDENTIFYING WMDP 12](#_Toc188947103)

[WMDPF TYPOLOGIES - DESCRIPTION AND ILLUSTRATIONS 14](#_Toc188947104)

[TYPOLOGIES – LINKS BETWEEN TF AND WMDPF, DESCRIPTION AND ILLUSTRATIONS 21](#_Toc188947105)

[GOOD PRACTICES: PREVENTION, COMBATING AND ELIMINATION (MITIGATION) OF WMDPF 25](#_Toc188947106)

# INTRODUCTION

The purpose and objective of this document is primarily to provide obliged entities under the Law on the Prevention of Money Laundering and Financing of Terrorism (AML/CFT Law) with experience gained from a broader international perspective, given that the matter of combating the financing of the proliferation of weapons of mass destruction (WMDPF) has its own long-standing experience, namely 2004 United Nations Security Council Resolution (UNSCR) No. 1540. This document can also help state authorities and institutions that actively participate in both the legislative and preventive-control aspects of combating the WMDP. The civilian sector should also not be neglected in terms of information, given that the matter of the WMDP and its financing is a potential global threat to world peace. The existence and development of WMDPF typologies (case scenarios), makes it easier for competent stakeholders (authorities, institutions) to combat the production, financing and proliferation of WMD. Typologies also provide insight and can contribute to the private sector (obliged entities under the AML/CFT Law) in easier identification and collection of relevant information (suspicious transactions) in the assessment of suspicious activities that are transmitted to competent authorities, thereby complying with their WMDPF prevention obligations.

This Typologies document looks at practices seen in the countries that have programs for developing capacities for the production of WMD, financial resources and developed logistics for supplying technology (brokers, intermediaries), equipment and dual-use goods (DUG). As for financing, i.e. movement of money, funds are usually transferred linearly (from the end user to the supplier through an intricate network of intermediary companies and financial institutions - banks) and there is no need for money laundering (ML). The situation is different when it comes to links between the financing of terrorism (TF) and WMDPF, where terrorist organizations (groups) have an interest in the proliferation of WMD, where money laundering of unknown origin is often present in order to acquire funds for terrorist activities. It rarely happens, but there are cases where individuals (usually experts and scientists) want to ‘sell their knowledge’ or certain equipment that can be used for the production of WMD. It should be added that the engagement of certain institutions – universities, which have the capacity to develop WMD, is also indicative.

The basic typological techniques of WMDPF involve the concealment of the beneficial owners (through front companies) of those involved in the business, both the producer (supplier) and the end user. Trade is diversified (vehicles, routes, transshipments), supply and deliveries are carried out through front entities, which are often offshore companies, with the participation of intermediaries (brokers, agents), with the most complex and multiplied (network) financing through numerous banks and jurisdictions. The contracted goods are usually dual-use goods that can often deceive the controls and the financial sector (banks) when they assess whether they are commercial-industrial goods or goods intended for the production and dissemination of WMD. The accompanying financial documentation is often misrepresented in order to conceal the authenticity of the goods.

Also, a presentation of the relationship between ML, TF and WMDPF can contribute to a better understanding of the matter in cases where they overlap.

An example of good practice is charting the path of good conduct and preventive measures, primarily for obliged entities under the AML/CFT Law, as well as when potentially making decisions on how to proceed in the event of suspicion on WMDPF.

# COMPARISON OF CHARACTERISTICS – MONEY LAUNDERING, TERRORISM FINANCING, PROLIFERATION FINANCING

A comparative overview below (Table 1[[1]](#footnote-2)) is provided in order to better understand the matter related to WMDPF, and to prevent certain doubts about the intertwining of sources and flows of money, participants in the business, and the purpose of the activities undertaken

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Money laundering** | **Terrorism financing** | **WMDPF** |
| **Sources of money** | From illegal activity | Internally from self-  funding cells (centered on  criminal activity)  Externally from  benefactors and fund-  raisers | State-sponsored programs |
| **Execution channels** | Favors formal  financial system | Favors cash couriers or  informal financial systems  such as hawala and  currency exchange firms | Favors formal financial  system |
| **Detection focus** | Suspicious transactions such as deposits inconsistent with the client's financial status or expected activity and clients (placement of money of unknown origin, layering and integration into legitimate economy) | Suspicious relationships,  such as wire transfers  between seemingly  unrelated parties | Individuals, entities,  states, goods and  materials, activities |
| **Transaction amounts** | Relatively high-amount transactions, often structured to avoid reporting obligations (to the bank) | Small amounts usually  below reporting  thresholds | Moderate amounts |
| **Financial activities** | A complex web of transactions that often involves front companies, bearer shares, offshore tax havens and shell (fictitious) companies | Varied methods including  formal banking system,  informal value-transfer  systems, smuggling of  cash and valuables | Transactions look like  normal commercial  activity, structured to  hide origin of funding |
| **Money flows (traces)** | Circular – money  eventually ends up  with the person who  generated it | Linear – money generated  is used to propagate  terrorist groups and  activities | Linear – money is used to  purchase goods and  materials from brokers or  manufacturers |

INDICATORS OF WMDPF, TABLE SHOWING HOW (FATF) INDICATORS WERE APPLIED IN CASES FROM INTERNATIONAL PRACTICE**[[2]](#footnote-3)**

When it comes to preventing and combating WMDP, the obliged entities under the AML/CFT Law, supervisors and enforcement authorities and the academic community tend to use indicators developed by authorities or institutions or by themselves (based on their knowledge and experience) as a starting point for undertaking actions under the Law and for assessing risks, vulnerabilities and threats or analytical studies.

This document aims to show how indicators have been identified and applied in practice through structured typologies and cases over the years since they were written and disclosed in relevant documents (guidelines, instructions). The focus will be on the 2008 FATF Typologies Report on Proliferation Financing.

Also, for the purpose of comparison with the above indicators, a list of FATF indicators from the FATF Guidance on Proliferation Financing Risk Assessment and Mitigation (June 2021) has been provided.

Why is it difficult to identify WMDPF?

One of the most difficult aspects of identifying proliferation is that the goods and materials involved are often industrial items that, if not clearly identified as subject to some type of control, may appear harmless to those involved in the supply chains and working in financial institutions and relevant regulatory authorities. Furthermore, most of the twenty possible indicators identified by the FATF are not uniquely linked to proliferation financing . They may also reflect trade-based money laundering (TBML), evasion of taxes or duties on shipments of goods, or other issues, such as incomplete trade documentation.

Analytical data relevant for this chapter is provided in Tables 2 and 3 below. The data is based on the Study of Typologies of Financing of WMD Proliferation, Final Report, 13 October 2017 Jonathan Brewer, King's College London.

The analysis is based on 60 case studies that vary depending on the quality and completeness of information provided by state authorities or financial institutions, or availability in court documents, UN committee reports, and media reports. Most of the information received from state authorities or financial institutions cover the last ten years. It is important to note that the studies involve countries that have proliferation programs. Most of them are covered by UNSC resolutions.

Although more than half of the case studies in the FATF 2008 Report related to trade financing such as letters of credit, such cases constitute a minority. This trend may reflect the development of proliferation financing, but may also be the result of inadequate data or the declining use of letters of credit in international trade.

**Table 2: Common characteristics in 60 analyzed cases of proliferation financing based on *the Study of Typologies of Financing of the WMDPF[[3]](#footnote-4)***

|  |
| --- |
| Involvement of front companies (either set up for the purpose, or adapted from an existing entity) or fictitious (shell) companies |
| Presence of citizens of countries involved in proliferation, i.e. persons with dual citizenship. |
| Involvement of low-volume companies, especially in brokerage and distribution activities. |
| The participation of universities in countries involved in proliferation activities, either as procurers or as financiers of procurement**.** |
| Using different channels (different entities, which may be geographically distant) to order, procure, and transfer goods and materials that may be related to proliferation. |
| Inclusion of companies whose products would be exempt from sanctions because they fall under the category of "humanitarian" provisions, for example food distribution companies . |
| Business or banking documentation contains neutral and non-specific descriptions of goods and materials, or the purposes of financial transactions. |
| Elaborate networks of cooperation with foreign countries, whether they existed before or were constructed for the purposes of proliferation. |
| Using personal bank or credit card accounts to purchase proliferation-related goods and materials . |
| Fast money transfer service providers process financial transactions on behalf of companies from sanctioned countries. |
| The turnover of goods and services is financed in cash. |
| Networks of companies that finance each other. |
| More fronts/fictitiouscompanymakes payments per invoice. |
| The company is carrying out business within an activity for which it is not registered. |
| Affiliated companies conduct transactions through multiple accounts at a single bank or financial institution to circumvent financial sanctions. |

**A. Elements that may indicate proliferation financing**

Listed below are also potential WMDPF indicators from the 2008 FATF PF typologies document.

1. Transaction involves individual or entity in foreign country of proliferation concern.
2. Transaction involves individual or entity in foreign country of diversion concern.
3. Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
4. Transaction involves individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
5. Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
6. Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
7. Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
8. Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
9. Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
10. Customer activity does not match business profile, or end-user information does not match end-user’s business profile.
11. Order for goods is placed by firms or individuals from foreign countries other than the country of the stated end-user.
12. Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
13. New customer requests letter of credit transaction awaiting approval of new account.
14. The customer or counter-party or its address is similar to one of the parties found on publicly available lists of “denied persons” or has a history of export control contraventions.
15. Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
16. Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
17. Transaction involves possible shell companies (e.g. companies do not have a high level of capitalization or displays other shell company indicators).
18. A freight forwarding firm is listed as the product’s final destination.
19. Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
20. Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

Table 3 below shows the relationship between the above indicators (FATF typologies from 2008) and cases – typologies that may indicate proliferation financing (analysis of 60 case studies). It is important to note that the indicators of importance of implementation and recognition of proliferation financing have been graded to HIGH, MODERATE and LOW LEVELS.

**Table 3.** Presentation of the gradation of indicators (A, B, C) in the typological cases of the above mentioned King's College study

|  |  |  |  |
| --- | --- | --- | --- |
| **Typology** | **Case typology indicator** | **Match with 2008 FATF indicator list** | **Note** |
| **Transactions that are potentially highly indicative of proliferation financing** | | | |
| A1 | Transaction involves individual or entity in foreign country of proliferation concern | Indicator 1 (number from the list above) | It may be a regular trade |
| A2 | Transaction involves individual or entity in foreign country of diversion concern. For example, a neighboring country or a country related to a country active in the WMDPF | 2 | It may be a regular trade |
| A3 | The persons involved in the transaction or their details (address, telephone number...) are similar to or possibly connected to entities that are subject to sanctions due to the WMDPF or are known to violate export controls. | 14 | It may be a regular trade |
| A4 | Presence of items controlled under the export of weapons of mass destruction or national control regime | Based on a case study | It may be permitted if consent is given. |
| A5 | Customer activity does not match the customer's business profile or information about end user do not match the end user's business profile | 10 | It may be a regular trade |
| A6 | The end user is not identified; for example, a shipping company or bank is listed as the recipient or final destination of the goods | 18 | It may be a regular trade |
| A7 | Involvement of an individual with ties to the country being linked to WMDP (for example, a person with dual citizenship); the person may be working with complex equipment for which they do not have the technical knowledge | Based on a case study | It may be a regular trade |
| A8 | The goods are ordered by natural or legal persons from other countries, not from the country where the (suspected) end user is located. | 11 | It may be a regular trade |
| A9 | Payments for industrial goods are made in cash. | Based on a case study | Rare in regular trade |
| A10 | The transaction involves the shipment of goods that are not compatible with the technical level of the country to which they are being shipped (e.g., semiconductor manufacturing equipment is shipped to a country that does not have an electronics industry) | 6 | It may be a regular trade |
| **Transactions that are moderately indicative for financing proliferation** | | | |
| B1 | Incorporation of shell or fictitious companies | 17 | It may be a regular trade |
| B2 | Small-scale trade through intermediary firms | Based on a case study | It may be a regular trade |
| B3 | The client is a manufacturer/trader of goods subject to export control. | Based on a case study | It may be a regular trade |
| B4 | The payment instructions indicate that it is a money transfer without a commercial transaction. | Based on a case study | It is unlikely that this is a regular trade. |
| B5 | Bookkeeping is organized in such a way that there is little obligation to record foreign trade transactions. | Based on a case study | It may be a regular trade |
| B6 | Customers and other counterparties to transactions are connected (for example, they share a common physical address, IP address, or telephone number ) or their activities are coordinated | Based on a case study | It may be a regular trade |
| B7 | Representatives of partner companies are connected by ownership or management structure | 16 | It may be a matter of regular trade; the participation of multinational companies. |
| B8 | Involvement of a scientific institution (university) in proliferation matters | Based on a case study | Scientific and research activities of academic institutions |
| B9 | In commercial or financial documentation, the goods are described as non-specific and harmless, or are described in a way that is misleading | Based on a case study | Local practice in certain parts of the world |
| B10 | Data and other items clearly indicate that the documentation related to delivery, customs, or payment is fraudulent. | Based on a case study | Other criminal activities |
| B11 | Using a personal account to purchase industrial goods | Based on a case study | It may be a regular trade (but it is not usual) |
| B12 | The transaction involves financial institutions known to have deficiencies in with their control systems in the field of preventing money laundering and terrorist financing and/or are domiciled in countries with weak export control regulations i.e. with weak implementation of regulations in the field of export control | 7 | It may be a regular trade |
| B13 | Bypass delivery routes, i.e. bypass financial routes transactions , especially through countries with poorly regulated financial systems | 15 | cost reduction , avoiding sanctioned entities or countries , war zones​ |
| B14 | The transaction involves the delivery of goods in a manner that does not conform to the usual geographical patterns of trade (e.g. does a particular country usually export/import a given type of goods?) | 5 | It may be a regular trade |
| B15 | The trade finance transaction involves a delivery route (if available) through a country with weak export control laws or weak enforcement of export control laws | 3 | It may be a regular trade |
| B16 | The transaction involves individuals or companies (especially trading companies) located in countries with weak export control laws or weak enforcement of export control laws | 4 | It may be a regular trade |
| **Transactions with low indicative value for proliferation financing** | | | |
| C1 | Based on the documentation obtained in the transaction, the declared value of the delivery is clearly reduced compared to the cost of delivery | 8 | Evasion of customs duties and taxes, money laundering through trade |
| C2 | The information in the trade documents does not match the financial flows, e.g. names, company names, addresses, destinations, etc. | 9 | Negligence in performing duties |
| C3 | The electronic payment form does not reveal the real purpose of the transaction | 20 | May be regular trade. |
| C4 | The client does not provide clear/complete information and is reluctant to provide additional information upon request. | 12 | Other criminal activities |
| C5 | A new client is looking for a job with a letter of credit while waiting for approval of a new account | 13 | May be regular trade. |
| C6 | A person not named on the original letter of credit or other documentation gives instructions for an electronic transfer or payment or such person is the recipient of the funds | 19 | Legitimate trade |

**INDICATORS OF POTENTIAL VIOLATION, NON-IMPLEMENTATION OR AVOIDANCE OF PROLIFERATION FINANCING – TARGETED FINANCIAL SANCTIONS***[[4]](#footnote-5)*

Following the chronology of creation and development of WMDPF indicators, below we provide a list of FATF indicators from its 2021 Guidance on Proliferation Financing Risk Assessment And Mitigation. Practical experience gained, new knowledge, regulation and prevention contribute to improving the assessment of the risk of proliferation in the private and public sectors. Certainly, as a starting point in risk assessment, indicators developed on a "realistic basis" and practically applicable can be a useful guide and risk assessment tool.

A risk indicator indicates or suggests the likelihood of unusual or suspicious activity. The presence of a single indicator in relation to a customer or transaction cannot in itself justify suspicion of proliferation financing, nor will a single indicator necessarily provide a clear indication of such activity, but it may prompt further monitoring and investigation as appropriate. Similarly, the presence of several indicators (especially from multiple categories) may also require closer examination. Whether one or more indicators suggest proliferation financing also depends on the business lines, products or services offered by the company; how the company communicates with its customers; and the company’s human and technological resources .

The indicators listed below are relevant to both the public and private sectors. As regards the latter, the indicators are relevant to financial institutions, natural and legal persons outside the financial sector and virtual asset service providers , whether they are small and medium-sized enterprises or large conglomerates. In the private sector, these indicators are intended for employees responsible for compliance, screening and monitoring transactions, analysis, accepting new clients and preventing financial crime.

In using these indicators, private sector entities should also consider the overall profile of the client, including information obtained from the client during the customer due diligence process; the way the business is financed and other relevant contextual risk factors. Some of these risk indicators do not necessarily relate to violations, non-compliance or avoidance of targeted financial sanctions , and are therefore not mandatory, but could be helpful to the private sector in understanding broader risks.

**CLIENT PROFILE RISK INDICATORS**

* During on-boarding, a customer provides vague or incomplete information about their proposed trading activities. Customer is reluctant to provide additional information about their
* activities when queried;
* During subsequent stages of due diligence, a customer, particularly a trade entity, its owners or senior managers, appear in sanctioned lists or negative news, e.g. past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes;
* The customer is a person connected with a country of proliferation or diversion concern, e.g. through business or trade relations – this information may be obtained from the national risk assessment process or relevant national CPF authorities;
* The customer is a person dealing with dual-use goods or goods subject to export control goods or complex equipment for which he/she lacks technical background, or which is incongruent with their stated line of activity;
* A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding;
* A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money-remittance business or a pay-through account. These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the activity associated with originators appear to be entities who may connected a state-sponsored proliferation programme (such as shell companies operating near countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls;
* A customer affiliated with a university or research institution is involved in the trading of dual-use goods or goods subject to export control.

**ACCOUNT AND TRANSACTION ACTIVITY RISK INDICATORS**

* The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern (i.e. DPRK and Iran);
* Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes;
* Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g. companies do not have a high level of capitalization or displays other shell company indicators.
* Countries or the private sector may identify more indicators during the risk assessment process, such as long periods of account dormancy followed by a surge of activity;
* Demonstrating links between representatives of companies exchanging goods, i.e. same owners or management, same physical address, IP address or telephone number, or their activities may be co-ordinated;
* Account holder conducts financial transaction in a circuitous manner;
* Account activity or transactions where the originator or beneficiary of associated financial institutions is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards or a weak export control regime (also relevant to correspondent banking services);
* Customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For financial institutions, the transactions are visible through sudden influxes of cash deposits to the entity’s accounts, followed by cash withdrawals;
* Transactions are made on the basis of “ledger” arrangements that obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies who maintain a record of transactions made on each other’s behalf. Occasionally, these companies will make transfers to balance these accounts;
* Customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business.

**RISK INDICATORS IN TRADE FINANCING**

* Before approving the invoice, the client requests a letter of credit (L/C) for a trade transaction for the shipment of dual-use goods or goods subject to export controls;
* Lack of complete information or inconsistencies in trade documents and financial flows, such as names, companies, addresses, final destination, etc.;
* Transactions include payment instructions or details by or to parties not identified on the original letter of credit or other documentation.

**Risk sectors for proliferation financing (FATF Guidelines 2021)**

Countries should be aware of which parts of the economy are subject to sector-specific UN sanctions, as these sectors would present a higher exposure to potential breach, non-implementation or evasion of PF-TFS. These sectors, as noted in recent UNSC reports, include, but are not limited to:

* **Trust and company service providers**: creating corporate entities that designated persons and entities use to obscure the links between a financial transaction and a designated person or entity; notaries public, other members of the legal profession and accountants providing trust services; use of fictitious and shell companies, legal entities with a formal owner and controlling body, legal entities or legal arrangements without obvious business reasons, company formation services;
* Dealers in precious metals and stones: providing an alternative method for designated persons and entities to surreptitiously move financial resources across international borders;(designated persons hire these traders to transport gold and diamonds in order to obtain foreign exchange to finance their transactions );
* **Virtual asset service providers :** providing products to designated individuals that have been "mined" and stolen, and providing a platform for rapid cross-border money transfers. As access to the formal financial system is increasingly closed to affected individuals due to the introduction of various financial sanctions, virtual assets are used to evade sanctions. This new method and technology for accessing financial services is particularly attractive to individuals and legal entities. persons covered by targeted financial sanctions for financing proliferation related to the DPRK, who encounter increasing obstacles in accessing banking services due to sanctions provided for by UNSC resolutions;
* **Maritime sector:** designated persons and entities also exploit the maritime sector, which provide them the means to deliver components and materials for use in WMD or their delivery systems, to illicitly engage in economic sectors in violation of the provisions of UNSCRs, the revenue from which can provide the underlying financing for a WMD programme;
* **Correspondent banking services**, though not always present a uniformly high-risk area, have been increasingly exploited by designated persons and entities as they often make use of international trade to conduct sanctions evasion activities;
* **Trade finance** is another example of service exploited by designated persons and entities. This is because PF sanctions evasion often involves cross-border trade of goods or commodities. While the majority of trade is done through open-account transfers, many also take place using trade finance instruments, which involve a financial institution acting as an intermediary, guaranteeing a transaction if certain documentary requirements are met by the counterparties to the transaction (exporter and importer). As a result, the financial institution receives significantly more insight into the details of the trade. Designated persons and entities who have to rely on trade finance instruments will do so fraudulently, using forged documents, misrepresenting the parties to a transaction, or arranging for a different end-destination or end-user from the one listed in the paperwork.

# TYPOLOGIES – DESCRIPTION, ILLUSTRATIONS, TRIGGERS FOR IDENTIFYING WMDP

Considering all of the above in terms of the application of the list of indicators (FATF) in typologically practical cases, it can be concluded that almost all cases (typologies) are mainly related to state programs for the development of WMD and the expansion of WMD financing. Cases of participation of individuals are very rare, and if this is the case, it is highly specialized individuals who offer partial equipment or dual-use goods (DUG) that they have acquired thanks to their position in WMD research and development, which they want to monetize. It is also possible to mention the non-dominant participation of academic institutions (universities) in WMD proliferation programs, but the sponsors of financing still remain states that are mainly recognized and sanctioned by UNSC resolutions. When it comes to the participation of terrorist organizations and groups, practice also recognizes presumed connections with designated (sanctioned) persons, whether from countries sanctioned by UNSC resolutions or not. Their interests are common, and if they finance proliferation, they use cash, precious metals, often legalized through third countries, or they abuse NPOs in the form of collecting money from donors-benefactors, or online donations.

If the transactions have the appearance of legitimacy, then they use front companies and fictitious companies with forged documents, while the sources of financial resources usually come from goods previously acquired through smuggling and "laundering" through "intermediate" countries.

Before listing typologies (typological cases), it is desirable to list important elements as triggers – *red flags for* increased attention and taking action in assessing whether the financing of the proliferation of weapons of mass destruction is involved.

**From the obliged entity's perspective, the initial triggers - red flags for increased attention would be those with the following characteristics:**

* Involvement of high-risk states in terms of proliferation financing (states designated under UNSC sanctions or, according to certain information, individual states are in some way connected to proliferation);
* The appearance of prohibited industrial goods and articles (materials), dual-use goods (DUGs) under the export control regime;
* The emergence of intermediaries (especially multiple intermediaries) for dual-use goods or prohibited goods (multiple sellers or buyers in the chain, to make it more difficult to identify the end user);
* Concealment or difficulty in identifying end users;
* Persons indicating connections to designated persons or sanctioned countries;
* Transactions of global significance that stand out due to their complexity and the way they are structured (time differences for related transactions, frequency, etc.);
* Correspondent banks involved for numerous intermediary companies (often fictitious or offshore);
* Procurement and shipping routes through countries with weak regulation or control for WMD and DUGs (often third countries);
* Geographical mismatch of the origin of goods, shipping or transshipment routes (a common case) in relation to regular trade;

It is also worth noting the following important elements when it comes to participants in proliferation financing:

**Individuals:**

* Individuals are often engaged in the procurement of proliferation goods;
* They hide behind dual citizenships and problematic national origins;
* They conceal their involvement and misrepresent themselves;

**Companies (participating firms):**

* Complex structure (registration, ownership);
* These are usually "front" and fictitious companies;
* Foreign citizens mostly appear on documents or in the company registration process;
* Multiple countries appear in one transaction (procurement, trade in goods, financing);
* They are located in countries with weak foreign trade controls, especially in the context of goods classified on export control lists (ECLs);
* They are located in the neighborhood of countries where the WMDPF is taking place or countries that cooperate with such countries.

The main questions that arise when it comes to WMDP are the following:

1. **What are the sources of funds and who finances proliferation?**

Experience in the fight against proliferation financing generally indicates that these are budgetary funds of states that have proliferation programs, less often funds from criminal activities of terrorist financing, organizations, groups, radical supporters that support the development and financing of proliferation. To a much lesser extent, it is possible to raise funds from donors, both natural and legal persons (NPOs) that support proliferation programs;

1. **Payments and cash flows**

In general, the purpose of the transaction on the way from the source (supplier/manufacturer) to the end user of the goods is hidden, intricate and complex. A normal - direct banking correspondent channel is possible, but is often routed through multiple economic entities and banks, especially when it comes to countries with secret programs or under sanctions;

1. **Suppliers, distributors and users of proliferation goods**

Manufacturers have equipment, technology or dual-use items (DUGs). Due to the threat of sanctions, direct export (sale) is often replaced by indirect trade in the form of suppliers (resellers) and intermediaries - brokers. As has been noted many times, the beneficiaries are states with proliferation development and expansion programs. The participation of designated persons who support WMD development and expansion programs is also not negligible; This concerns biological-chemical, nuclear-radiological and dual-use goods (DUGs).

**Considering the above, the applied techniques used in financing proliferation can be identified:**

* Diversification of financing and trade to avoid identification by competent authorities and institutions;
* The presence of front companies aimed at facilitating the proliferation and financing of WMD;
* Falsification of trade and financial documentation;
* Structuring (arranging) the necessary financial resources to finance trade or intermediaries (branches) in various countries;
* Manipulation of source information (removal, changes, etc.).

It is less important for financial institutions (or obliged entities), but it is worth mentioning manipulations in container transport, road transport (changes in container numbers, vehicle names, registration, etc.)

WMDPF TYPOLOGIES - DESCRIPTION AND ILLUSTRATIONS

**FATF TYPOLOGY**

Fictitious - front companies in an WMDP network

A standard typology that is often cited in many documents of financial intelligence services of states and competent authorities dealing with the issue of proliferation of weapons of mass destruction: FATF "Report on Proliferation Financing" from 2008.

Transportation

​ goods

goods

Front company

Importer

Exporter

Broker

$ $ $ $

Broker’s bank

Exporter’s bank

Importer’s bank

$ $

Below are typologies describing possible events (participants and commodity and financial flows) in the processes of proliferation of weapons of mass destruction.

1. WMD PROLIFERATION AND ITS FINANCING THROUGH INTERMEDIARY - FRONT COMPANIES AND BROKERS

The typology shows the basic way of financing the proliferation of WMD, which is reflected in the complexity of the delivery of ordered goods and financing (payment). The goal is to create a complex network of commodity-monetary transactions with the intention of concealing the source - the origin of the goods and the supplier (producer) and the real user (end user) of equipment, technology or dual-use goods (DUG). In order to achieve this intention, front companies are used that have the task of mediating in the business and concealing the real participants in the business, more precisely the real owners of the companies. The presence of brokers (commodity intermediaries) is common in order to stratify the goods from the supplier to the end user. A complex financing network, which involves numerous financial institutions, primarily a chain of combined banks from legitimate, quasi-banks to offshore banks. The transport of goods often has "complex lines" (routes), transshipments and combined transport (sea, air, road, rail).

Transport of goods

(sea, road, rail)

potentially combined)

Supplier,

Manufacturer

Broker

Front company

Importer,

End user

Payment bank (chain) of the supplier / importer – end user, exporter, broker

Bank

Bank

Importer’s bank

Bank -offshore

Payment for goods

2. COMPLEX PROLIFERATION NETWORK (UNKNOWN MANUFACTURER AND END USER, COMPLEX FINANCING NETWORK)

Typology number 1 provides a basic example of WMD proliferation. Depending on the current situation regarding proliferation, and considering the existing circumstances in regulation, prevention and combat, participants behave accordingly. Practice has shown that when it comes to proliferation programs of sanctioned states, as well as the participation of designated (sanctioned) persons, the business is “complexly networked”, as this typology shows. The large number of intermediaries in the business (intermediaries) and structured financing through a multitude of banks in the chain make it difficult to detect proliferation financing. Transactions are structured in such a way that they are numerous, often do not follow the flow of goods in time (advance payments, delayed payments beyond deadlines, etc.), and the basis of payment is questionable. Delivery is often accompanied by false and questionable documentation on the origin and authenticity of the goods.

Transport of goods (proliferation)

Possible mixing

Front company

Exporter - supplier,

Manufacturer (one or more)

End user

Importer

Complex ownership structure

Sale

Broker

Front company

Front company

financing

A complex network of financing

A network of banks, importer, end user, front companies, brokers, exporters (if goods were purchased from manufacturer), manufacturer of goods for proliferation (may be exporter too). A combination of regular banks, offshore companies and transfer of funds through offshore and fictitious firms in order to conceal the source of payment.

3. PROLIFERATION THROUGH BARTER ARRANGEMENTS (SETTLEMENT BY EXCHANGE OF GOODS)

The typology illustrates the proliferation of dual-use goods (DUGs) that can be used in both industrial and commercial purposes, i.e. they are subject to normal trade, but they may also be subject to an export licensing regime. For repressive and preventive authorities and institutions, there is a problem of actual identification of DUGs intended for the spread of proliferation. "Mixed" deliveries of goods intended for proliferation (DUGs) are possible, mixed with industrial and commercial goods, but tariffed as commercial, with often falsely described goods (false documentation). Concealment of manufacturers, original suppliers (actual owner of the goods) and end users of the goods is standard.

Bartered goods buyer

Selling goods through barter

€ link €

Intermediary (broker, agent)

Front company

End user (proliferation country, designated persons)

Supplier, manufacturer

Barter

link link exchange

Transport of goods potentially mixed (DUGs for proliferation + commercial goods)

DUGs DUGs

4. COMPLEX ROUTES OF SHIPPING GOODS WITH TRANSSHIPMENT AND RE-DIRECTION IN NUMBER OF DIRECTIONS

In addition to the basic methods of spreading and financing proliferation listed in the previous typologies, this typological case highlights the complexity of delivering goods in order to conceal the origin of the goods, and consequently the origin of funds through complex money flows (interconnections). The upper part of the illustration shows a complex flow of goods that has a complex path (route) from shipment to receipt. Goods en route (especially by sea) due to a long journey can become the subject of purchase and sale because the bills of lading (ship bills of lading) are a kind of security and can be transferred to other holders (owners), which further complicates the discovery of the origin of the goods. Transshipment in a jurisdiction with weak control of goods and the redirection of goods through unnecessary and roundabout routes with extremely questionable accompanying trade documentation further complicates the identification of the origin, as well as the goods themselves. Cash flows tend to be "convoluted and intricately structured."

Transshipment – country with weak import controls

Normal routes are changed to conceal origin of goods

redirection

goods

Shipping of goods (combined transport)

Possible sale of bill of lading ( B/L )

goods

Agent for the goods user

End user – proliferation program

Supplier

Front company

agent-broker

€ € €

Many financial intermediaries (banks) in payment chain; complex transactions, numerous, often fictitious

€ €

Bank

Bank

5. PROLIFERATION THROUGH INTERMEDIATE COUNTRIES

The typology depicts the intermediary country (B) as an intermediary in the implementation of the proliferation program of country A. These are often countries that support the development of proliferation for reasons of militarization, geopolitical interests, or radical-terrorist attitudes and support.

Country A Country B Country C

proliferation program intermediary supplier

Front company

broker

broker

Order order

link

bank

Order

Company –comm. business

Broker – supplier

Manufacturer - supplier

Goods (mix) goods

Prolif; commerce. Prolif.+ commercial

€

payment

bank

bank

bank

6. NUMEROUS PARTICIPANTS IN PROLIFERATION: MANUFACTURERS, SUPPLIERS, CONTRACTORS, FINANCIAL INSTITUTIONS

The typological case shows the complexity of the ordered proliferation business in terms of procurement, delivery and payment. The typology takes the example of dual-use goods (numerous DUG items), which is a good basis for creating a network of participants through front companies, as clearly shown in the illustration. Such a complex diversification of the flow of goods greatly reduces the risk of detection and seizure of goods due to the large number of suppliers of goods, usually front companies that otherwise conceal the real participants in the business (owners) and the legitimacy of the business. Money flows move through offshore zones through fictitious companies or often through foreign legal entities (trusts) with the mediation of numerous banks, which complicates the identification of the origin and flows of money. Due to the complexity of the business, the participation of a coordinator of the business (usually a person of questionable reputation, dual citizenship, non-resident) is also possible, and it may also be a person with expert knowledge in the field of proliferation (scientific and research personnel).

Ordering party - proliferation program

Front companies – a number of them contracts with suppliers and manufacturers (several of them)

DUG order

(business – financial connection )

DUG cash flow €

natural person – potential

Trusts offshore firms - often

Offshore areas fictitious

cooordinator

Many front companies in delivery chain

due to complexity

Many suppliers - (DUG) from many countries

DUG

Many banks

€

7. PROLIFERATION FINANCING THROUGH EXCHANGE OFFICES AND NON-PROFIT ORGANIZATIONS (NPOs)

The typological case indicates the support of sympathizers and supporters of proliferation and financing of proliferation, individuals and legal entities who support proliferation programs through a network of exchange offices or through NPOs. In this case, the main flow of money is cash, so in this case the money changers are exposed to risk. In the case of NPOs, proliferation programs are possible disguised as charity, often unknown to donors, whereby donors “unknowingly” finance proliferation.

Designated persons: individuals and entities (proliferation or supporting program)

Country „А“ with proliferation program

Link - interest

€ € €  €

NPO – various purposes

Exchange offices of country “А“ (or neighb. country)

donations

Regular legal entities and individuals (residents, non-residents, foreign persons)

8. UNKNOWN INVOLVEMENT OF REGULAR FIRMS WITH COUNTRIES UNDER SANCTIONS OR DESIGNATED PERSONS OR WITH COUNTRIES KNOWN TO HAVE PROLIFERATION PROGRAMS

Due to the lack of "good practice" among obliged entities (primarily financial institutions), omissions are possible that can contribute to "unconscious" proliferation, and thus to a worse reputation. In addition to banks, companies with a good reputation can also make a mistake, especially if a partner gives them "on the spot" suspicious and unusual orders for transferring funds.

Country under sanctions or with proliferation program; designated persons

Offshore firms; front, fictitious

Bank with reputation

transfer transactions

numerous bases

link

possible link?

Bank client

9. INVOLVEMENT OF NATURAL PERSONS AND SCIENTIFIC RESEARCH INSTITUTIONS IN PROLIFERATION

Practical experience indicates that certain individuals from the scientific and research community, as well as scientific and research institutions, want to monetize their knowledge or proliferation-sensitive items by cooperating with countries under sanctions or designated persons. As in all the above typological cases, there is a concealment and multiplication of money and goods flows through intermediaries (front companies) and a network of banks.

Front companies in multiple countries for shipment of goods

Scientist – researcher,

Scientific research institutions (universities)

Country under sanctions, with proliferation program; designated persons

Goods goods

proliferation

€ €

Complex financing network, multiple banks, often payment through offshore entities, structured transactions

Banks, offshore areas

€

10. COMPLEX GOODS STRUCTURE (COMMERCIAL, DUAL-USE GOODS - DUG) AND TRADE DOCUMENTATION (REAL AND FICTITIOUS)

Trade financing is a series of actions taken to ensure the execution of a contracted business. It is a kind of guarantee that the supplier will receive his money, and the customer will receive the goods. Certainly, a significant part of these activities relates to trade and financial documentation (invoices, bills of lading, specifications of goods and packing lists, etc.)

In order to conceal dual-use goods that are under the export license regime and can be used for proliferation, and which can also be recognized as goods for industrial-commercial use, false shipping and accompanying documentation is created (false tariff of goods, invoices, specifications of goods, waybills, etc.) with the aim of presenting numerous items shipped under the DUG regime as industrial-commercial goods in order to circumvent the envisaged sanctions. Often, goods are mixed (DUG + commercial) and moved through a transit country or through several of them to numerous regular companies (possibly front companies) in order to diversify and reduce the risk of delivery due to the threat of potentially possible seizure of the DUG or individual items (under the export license regime), if they are discovered during transport to the final destination. Upon arrival, the DUG is directed towards implementing the proliferation program.

Deliveries via intermediary country

Commercial goods; sale, distribution

(all companies in one country) – possibly more

intermediate countries)

Legitimate companies (having an activity), several firms in delivery transaction

Country of origin of DUG + commercial goods

Importer –broker or end user

goods DUG

€ €

Proliferation development (program)

DUG

TYPOLOGIES – LINKS BETWEEN TF AND WMDPF, DESCRIPTION AND ILLUSTRATIONS

The four (4) typologies listed, described and illustrated below show the connection between the financing of terrorism and the financing of proliferation as a global threat to peace and stability. Terrorist organizations and groups or individual terrorists will certainly financially support programs and activities for the development of proliferation if this fits into the achievement of their radical goals, which is opposed to the constitutional order and policies of states, and threatens the security of the civil community or certain groups of people or individuals. It is difficult to identify transactions related to the financing of terrorism (FT), because legal financial institutions are bypassed, and if this is already present, this phase was preceded by "laundering" of illegitimately acquired funds (smuggling of precious metals, various types of serious crime). A milder and somewhat legitimate method can be associated with collecting funding sources through non-profit organizations (NPOs), although their abuse is not excluded.

1. TF AND PF THROUGH SMUGGLING OF PRECIOUS METALS

The typological case shows the financing of terrorism (TF), terrorist organizations, terrorist groups in the usual way for terrorism, by extracting (mining) precious metals (gold, silver, platinum, etc.) and smuggling with the aim of legalization for further sale and realization of financial means for terrorist and proliferation activities. The illustration clearly shows the flow of smuggling of goods (precious metals) that are "laundered" and legalized in country "C" become the subject of export to country "D" where processing is finalized and sale is carried out. The funds obtained usually go to the hands (in cash) of terrorists or legitimate transfers of smaller amounts are made (below the reporting threshold of obliged entities under the AML/CFT Law). The acquired money is used for terrorist activities and as support for a sanctioned country for the development of proliferation. A connection with "designated persons" or persons who support WMD proliferation programs is also possible.

Country "A" Country "B" Country "C"

Precious metal mines or handling of precious metals

Sanctioned – proliferation program

Change of origin of precious metals

smuggling

precious metals

Fin. proliferation

link (support) export

Country "D"

Precious metal processing (refinement) and sale to buyers

Terrorist organizations and groups exploit and control precious metal market

Support to designated persons and those supporting proliferation

indirect financing

support for terrorism

Individuals – cash couriers

2. THE ROLE OF NON-PROFIT ORGANIZATIONS (NPOs) IN FINANCING PROLIFERATION – SUPPORT TO "DESIGNED PERSONS" AND INDIRECTLY TO COUNTRIES WITH A PROLIFERATION DEVELOPMENT PROGRAM

The typological case and illustration presents the role and possible misuse of NPOs in raising funds for the financing of terrorism and indirect financing of the proliferation of WMD. An NPO can attract a high number of donors (investors) with its program, depending on the program of activities. Possible misuse is reflected in fictitious programs that can deceive the general public – donors (investors) into thinking that they are doing a good deed, and not financing terrorism. Through further activities, the NPO finances “designated persons” and indirectly a country with a proliferation program through money transfer couriers.

Country "A" Country "B"

Terrorist organisation; group

Designated persons; persons involved in proliferation development

Proliferation program development

funding of connections

financial

support

Donors; individuals and entities

NPO (as front – association) for raising funds

donations

cash financial assets

couriers

account

Investment in legitimate business as lasting source of funds

Part of the funds for NPO program activity

Note: NPO programs

1. Fictitious (disguised/fake)
2. Actual programs to fund NPO activities (in the service of concealment and as cover for financing proliferation)

3. THE ROLE OF FRONT COMPANIES IN THE FINANCING OF TERRORISM (FT) AND PROLIFERATION

By disguising the real participants (owners) while maintaining the presence of a legitimate business, a front company conceals or carries out the illegitimate activities of the participants in such businesses. The “front” companies convert smuggled precious metals (or other valuable goods) into investment assets that generate income and profit and invest them through legal transfers in an NPO that is associated with terrorist organizations or groups that support WMD proliferators.

Country "A" Country "B"

Processing –sale - investment

Terrorist organization and designated persons

Front company 1

NPO

smuggling

of precious metals

Front company 2

link donations

founder (shareholder, owner of shares)

Country "C"

Transfers : profit, dividend,

Income from mutual business

Front company 3

4. TRADE FINANCING OF PROLIFERATION THROUGH FICTITIOUS DOCUMENTATION

As stated in Typology 10, trade finance is a set of actions taken to ensure the performance of a contracted business. It is a kind of guarantee that the supplier will receive his money and the customer will receive the goods. Certainly, a significant part of these activities relates to trade and financial documentation (invoices, bills of lading, specifications of goods and packing lists, etc.)

In order to conceal dual-use goods (DUG) for terrorist activities that are under the export license regime and can be used for proliferation, and which can also be recognized as goods for industrial-commercial use, false shipping and accompanying documentation is created (false tariff of goods, invoices, specifications of goods, waybills, etc.), with the aim of presenting numerous DUG (proliferation) shipping items as industrial-commercial goods in order to circumvent the envisaged sanctions. The goods are moved through a transit country and in partial deliveries to numerous companies (possibly front companies) in order to diversify and reduce the risk of delivery due to the threat of potentially possible seizure of DUG or individual items (under the export license regime) if they are discovered during transport to the final destination.

Country "A"

Country of DUG origin + commercial goods as 'mask’ (mixed delivery)

Transit country "B" goods

Legal (regular) companies

4

3

2

1

goods

Country "C" with a proliferation program and a "sponsor of terrorism"

Proliferation program

Importin company

Purchaser of commercial goods for processing or sale

Terrorist org group; receipt of DUG for proliferation program and link to designated persons

Designated persons

# GOOD PRACTICES: PREVENTION, COMBATING AND ELIMINATION (MITIGATION) OF WMDPF

Taking into account all the above, described and illustrated, there is a need to point out, primarily to obliged entities under the AML/CFT Law, good practice in the application of preventive measures and the fight against the financing of the proliferation of weapons of mass destruction. There is certainly room for improving good practice measures depending on the nature of the business and the risk exposure of the private sector – obliged entity.

In order to review and "recommend" good practice, a comparison of good and bad practices in counter-proliferation from a broader perspective is provided.[[5]](#footnote-6)

**Good and bad practices for preventive measures and combating proliferation financing:**

Consideration by the competent authorities of a broader aspect of prevention and fight in relation to the perspective of obliged entities under the AML/CFT Law.

|  |  |
| --- | --- |
| **Examples of good practice** | **Examples of bad practice** |
| Screening information (verification, monitoring) is contained in trade documents against applicable sanctions lists | Employees working on sanctions issues in the economy are not qualified and experienced to perform the function effectively. |
| The results are investigated before proceeding with transaction (for example, obtaining confirmation by third parties that the person is not sanctioned o ) and clear documentation explanations for all decisions made | Failure to review trade documentation, undocumented decision-making |
| Shipping container numbers are checked based on sensitive risks | Failure to carry out checks against all relevant international sanctions lists |
| Phased (staged) verification of transactions to check compliance with potential sanctions | Failure to update information regarding changes to the names of sanctioned persons, particularly as these changes may not be immediately reflected on the sanctioned persons lists |
| Previous sanctions warnings are analyzed to identify situations in which a match is most likely to occur and the bank is focuses its resources on sanctions accordingly | Failure to record the rationale for the decision to reject false positive results |
| New or changed information is recorded and checked. | Failure to verify data about agents, insurance companies, shippers, freight forwarders depending on the risk; about delivery agents, inspection agents, signatories, and the parties specified in the certificates of origin, as well as the main contracting parties in the transaction |
|  | Failure to record the reasons for decisions not to inspect certain entities and to retain that information for control purposes |
| Ensure that employees are aware of the issues related to dual-use items, common types of dual-use goods and to be able to identify red flags that suggest that there is a risk that dual- use items may be delivered for unauthorized purposes | Lack of a clear policy on dual-use items |
| Confirmation (compliance) with exporters in higher risk situations whether a state permit (license ) is required for the transaction and requesting a copy of the permit (license) where necessary | Failure to undertake further investigation in cases where the description of the goods is unclear or unspecified |
|  | Third -party data sources are not used where checks on dual-use items are possible. |

**Proposal for good practice**

From the perspective of obliged entities under the AML/CFT Law, it can be briefly said that good practice would at least include the following:

**Responsibility in terms of preventing and combating the financing of proliferation:**

* Introduce (adopt) internal procedures and policies for UN targeted financial sanctions: This means introducing or adapting policies and procedures to reflect the risks posed by WMD proliferation or the financing of WMD proliferation.

**Introduce (adopt) preventive measures:**

* **Risk Assessment** : Conduct and document an appropriate business risk assessment, specific to the individual business, to identify the degree and type of exposure to WMD proliferation and WMD proliferation financing risks. Business risk assessments should be regularly reviewed and updated ;
* **Strengthening customer due diligence measures** : This includes a broader view of customers in terms of proliferation. Relationships include customers and other contractors (e.g. manufacturers, suppliers, consultants or agents) whose activities may carry a risk of involvement in proliferation and/or financing of WMD. With respect to contractors, consideration could be given to including clauses in contracts relating to compliance with proliferation and financing laws. The degree of risk of any customer, country/jurisdiction, transaction, product/service, distribution channel, other contractor, transshipment location and association with states subject to proliferation/financing of WMD sanctions affects the risk profile of the customer relationship or other contractual relationship .
* **Understanding the actual ownership of relationships and assets is very important and financing relationships and transactions** . Beneficial ownership refers not only to the amount of the share, but also to the control of the company and business relationships;
* **Analytical assessment of suspicious activities** : modification (updating) and application of indicators, studies and development of typologies as a manual, development of strategic analyses as a reflection of the recognition of the situation and events "on the ground", matching the applied indicators with the risk assessment - "realistic case scenario";
* **Internal control activity** : establish basic controls with a special focus on dissemination and dissemination financing. Real-time activities, not “post festum”- with a delay;
* **Audit familiar with activities in the fight against proliferation** : tasked with objectively reviewing adopted procedures, assessing proliferation risks, analyzing the work of internal control and confirming with their conclusions the adopted documents, actions and measures in the field of prevention and fight against proliferation financing;
* **Continuous employee training** : the need for employees to be aware of the risks related to proliferation and proliferation financing activities that they may encounter in their business. Staff should be provided with appropriate and regular training, information and resources to improve their understanding of proliferation and proliferation financing, including techniques used to avoid detection and indicators, increase their awareness of relevant legal obligations , including the need to check for any activities that may constitute a breach of relevant sanctions regimes. Ensure that they are able to effectively implement risk management or risk mitigation procedures, and know where to seek further information or guidance when needed .
* **Corporate governance approach to proliferation** : the legal committee or equivalent governing body should regularly review compliance with legal obligations relating to proliferation and financing of proliferation . WMD as part of compliance with the sanctions regime, as well as to assess the extent to which business policies, procedures and controls are met. Obliged entities (the real sector) have long been subject to legal obligations regarding expansion and financing of expansion The WMU and their leadership should in any case monitor compliance with these obligations.

1. Taken over from the Study of Typologies of Financing of WMD Proliferation, Final Report 13 October 2017 , Jonathan Brewer, Kings College London). The related footnote indicates that this table was based on a presentation by James R. Richards (Wells Fargo, 2005), cited in the CAMS Examination Study Guide 57th Edition, and that the author of that study added a right-hand column to this presentation titled WMD Proliferation Financing.

   However, some fields in the ML column have been slightly amended for clarity [↑](#footnote-ref-2)
2. Brochure: “Assessing the Risk of Financing Weapons of Mass Destruction” [↑](#footnote-ref-3)
3. Study of Typologies of Financing of WMD Proliferation, Final Report of 13 October 2017, Jonathan Brewer, King's College London [↑](#footnote-ref-4)
4. Taken from FATF *Guidance on Proliferation Financing Risk Assessment and Mitigation,* June 2021 [↑](#footnote-ref-5)
5. Source: Jersey Financial Services Commission - Guidance on Countering the Financing of Proliferation of Weapons of Mass Destruction , April 2022 [↑](#footnote-ref-6)