Black Sea Trade & Development Bank

Policy on Anti-Fraud, Corruption, Money Laundering and Terrorism Financing, and Domiciliation of BSTDB Counterparties

Table of Contents

1 Purpose & Scope

The fight against fraud, corruption, money laundering and financing of terrorism ("FCMLTF") represents a necessary and important component of the mission of the Black Sea Trade and Development Bank ("the Bank") to promote regional economic development and co-operation. Additionally, the Bank is committed to respect international standards with regard to the proliferation of weapons of mass destruction (WMD) as well as United Nations Security Council sanctions and contractual undertakings of the Bank.

In the spirit of the Agreement Establishing the Bank and according to its policies and international best practice, the Bank wishes to establish policies, procedures and systems of internal control, which may be revised from time to time, to address the risks arising from FCMLTF.

The Bank is committed to ensuring that the risks of FCMLTF are reduced to the lowest possible levels, both internally and in its dealings with external parties. Where there is the possibility of FCMLTF, the Bank will deal with it in a decisive, timely and controlled manner.

Within this framework, the Bank:

a. has developed this Policy and associated procedures, and

b. is committed to working and co-operating with other organizations to prevent FCMLTF. Wherever possible, the Bank will seek to co-operate and exchange information with peer Institutions, the relevant competent authorities of its Member States and with competent international organizations, in order to assist in combating FCMLTF, primarily within the region of its operations.

The Bank expects all its Officials, Staff Members and counterparties, including its consultants, contractors, and customers- to observe the highest standards of ethics and to provide the Bank with any help, information and support in combating FCMLTF.

The purpose of this Policy is to outline the Bank's role in preventing and combating FCMLTF and reducing the related risks to the lowest possible level in its activities.

Through a combination of working with the authorities in countries of operations and undertaking focused due diligence on individual clients, the Bank can be a force for positive influence at the systemic level and, at the same time, avoid exposure to unnecessary risks in individual operations. Furthermore, this approach could enable the Bank to play a role in the international and regional effort against money laundering and terrorism financing.

2 Terms & Abbreviations

2.1 Terms

The following terms are used in this policy as respectively defined below:

- **Bank:** the Black Sea Trade and Development Bank
- **Bank Officials:** the President, the Vice Presidents and the Secreatry General
- **Board Officials:** Directors, Alternate Directors, Temporary Alternate Directors in their capacity as members of the Board of Directors
- **FATF Members:** the jurisdictions and regional organizations participating as members in the Financial Action Task Force (FATF)
- **Headquarters Agreement:** the Headquarters Agreement between the Government of the Hellenic Republic and the Black Sea Trade and Development Bank signed on 13th August 1998.
- **Management:** Bank Officials
- **Member States:** the Black Sea Economic Cooperation participating states that have become members of the Bank
- **Officials:** Board and Bank Officials

- **Staff Members:** Officers and staff of the Bank
- **Supervision and Monitoring:** the stage covering the period between the effectiveness of a public sector operation- or disbursement of a non-public sector operation- and the completion of the operation (or termination of a revolving facility).
- **Prohibited Practices:** fraudulent, obstructive, collusive, coercive and/or corrupt Practices

2.2 Abbreviations

The following abbreviations are used in this Policy

Abbreviation	Full Wording of Abbreviation
ALCO	Assets and Liabilities Committee
BoD	Board of Directors
CDD	Customer Due Diligence
DCR	Compliance and Operational Risk Management Office
DIA	Internal Audit Department
DGC	Office of the General Counsel
EDD	Enhanced Due Dilegence
FATF	Financial Action Task Force The Financial Action Task Force ("FATF") is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions [on the initiative of G7]. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas and is considered to be the globally leading anti-money laundering and terrorism financing institution
FCMLTF	Fraud, Corruption, Money Laundering and Terrorism Financing
FIU	Financial Intelligence Unit
FSA	UK Financial Services Authority
Global Forum	Global Forum on Transparency and Exchange of Information for Tax Purposes The Global Forum is the continuation of a forum which was created in the early 2000s in the context of the OECD's work to address the risks to tax compliance posed by tax havens. The original members of the Global Forum consisted of OECD countries and jurisdictions that had agreed to implement the international standard for transparency and exchange of information on request for tax purposes. The Global Forum was restructured in September 2009 in response to the G20 call to strengthen implementation of the standard.
IT	Information Technology
IU	Information Unit
KYC	Know-Your-Customer
MLTF	Money Laundering and Terrorism Financing
WMD	Weapons of Mass Destruction
OECD	Organization for Economic Cooperation and Development
PEP	Politically Exposed Person
SEC	US Securities and Exchange Commission
UBO	Ultimate Beneficial Owner

3 Responsibilities

The following Business Units and Positions are responsible for the corresponding tasks, as described in detail in the present Policy:

- **Each Member of the Bank's Management Committee** (Bank Officials):

  Has primary responsibility for the proper implementation of this Policy in their respective Division, for ensuring the integrity of the assets of the Bank. They must ensure, through regular control and risk self-assessments, that suitable controls to prevent FCMLTF are in place and that their effectiveness is monitored by regularly reviewing and assessing key risk indicators and qualitative factors.

- **The Bank's Audit Committee, DCR, DIA and its external auditors:**
  Shall enable Management to prevent and detect these threats within the framework of their responsibilities, as appropriate.

- **DCR:** has the responsibility to: i) prepare appropriate Know-Your-Customer (KYC) Procedures, ii) to provide guidance and consultancy to the operation teams on KYC and integrity-related/KYC issues, mainly during the Customer Due Diligence (CDD) and Supervision and Monitoring stages of an operation, as per the KYC Procedures, iii) upon request assist the Information Unit (IU) and Credit/Management Committee with integrity-related/KYC issues, iv) report any issues to the Audit Committee upon a relevant request and v) to regularly organize Board of Directors, Management and employee AML/CTF training programs, vi) review periodically the application and effectiveness of the present Policy, taking into account the international best practices in the prevention and combat of AMLCTF, as well as experience acquired through the implementation of the Policy and market practices on the subject, in order to update it, as required, vii) review periodically compliance with the present Policy, viii) monitor FCMLTF and KYC-related quantitative data in a practicable manner, so as to report it to the Management and upon request to the Audit Committee, as appropriate.

  In respect of the Domiciliation of BSTDB Counterparties rules, DCR is primarily responsible for assessing the operations' sound business reasons and the jurisdictions involved vis-à-vis their Financial Action Task Force (FATF) and Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) status.

  In particular, DCR is responsible for assessing the sound business reasons for the use and selection of a jurisdiction other than that where the project is located and include such assessment in the related approving documents. If there are important lingering uncertainties, and following a step of additional internal consultations with the Operation Team/Treasury and DGC, the respective Committee of the Bank [Credit or Assets and Liabilities (ALCO)], depending on whether the relevant transaction is a Banking or a Treasury one, could be asked to authorize external tax expertise to be sought ad hoc, prior to the eventual submission to the relevant Committee of the overall proposed transaction. For the inclusion of the relevant input regarding the existence of sound business reasons into the respective documents submitted to the appropriate Committee of the Bank for approval of the proposed transaction, the transaction team, DCR and DGC shall co-operate, as appropriate.

- **DIA:** plays an important role in independently evaluating the risk management and controls, discharging the responsibility of the Audit Committee of the Board of Directors through periodic evaluations of the effectiveness of compliance with policies and procedures, including related staff training.

- **Staff Members**: For the effective countering of the threats of AMLCTF, Staff Members have to take responsibility for their prevention and detection. In particular, Staff Members of Banking and Treasury should adhere to the requirements of the KYC and the Domiciliation of BSTDB Counterparties rules.

- **Information Unit (IU)**: has the responsibility of maintaining and updating the Bank's comprehensive and electronically searchable database with the names of all Bank's Banking and Treasury counterparties along with all related physical and legal persons provided for in the KYC Procedures, as submitted by the Operation

Teams during the KYC Due Diligence and Supervision and Monitoring stages and upon any change. The IU is providing its findings to the Operation Teams, maintaining complete and updated records of such findings.

Implementation

The implementation of this Policy will commence immediately after its approval by the Board of Directors.

4 Policy

4.1 IMPACT OF FRAUD, CORRUPTION AND MONEY LAUNDERING ON ECONOMIC DEVELOPMENT

It is widely accepted that both fraud and corruption hinder economic development, inter alia for the following reasons:

a. they are anomalies that degrade the performance of the economic system as a whole and harm a country's or region's long-term economic efficiencies;
b. they cause mistrust among communities, hence hinder economic cooperation and development;
c. they increase the cost of the development process;
d. they diverge the allocation of scarce resources into unnecessary, uneconomic or illicit uses;
e. they create economic instability and divert foreign investments to more stable economies;
f. they lower asset life, as resources are directed away from maintenance toward new equipment and projects;
g. costs of fraud and corruption are often borne disproportionately by the poor, while the "gains" are skewed towards the rich, the powerful, and the politically well-connected;
h. corruption and fraud undermine laws, create disrespect for values, rules and perceptions of unfairness
i. in economic terminology, fraud and corruption increase transaction costs in an economy, increase real and perceived risks for undertaking economic activity and generate a 'dead weight loss' which increases inefficiency.

Moreover, laundered money provides drug traffickers, organized criminal groups, arms dealers and other criminals with the wherewithal for operating and developing their enterprises. The activities of powerful criminal organizations can have serious social consequences. Furthermore, without effective safeguards or preventive measures, money laundering can strike at the integrity of a country's financial institutions. The removal of billions of dollars from legitimate economic activities each year constitutes a real threat to the financial health of countries and affects the stability of the global marketplace.

Money laundering undermines international efforts to establish free and competitive markets and hampers the development of national economies. It distorts the operation of market transactions, may increase the demand for cash, render interest and exchange rates unstable, give rise to unfair competition and considerably exacerbate inflation in the countries where the criminals conduct their business dealings.

4.2 PREVENTION OF FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING

4.2.1 Managing the Risks

The Bank shows 'zero tolerance' to FCMLTF. In order to counter FCMLTF it is best to prevent it from happening in the first place. That is why the Bank deems essential to have clear policies and procedures and an ethical, control-awareness culture, within which: a) the Bank's governing bodies, Bank Officials, Staff Members, experts, consultants and contractors can work and b) its financing operations and other activities may be conducted.

The management of FCMLTF prevention should stem from the Bank's control and risk awareness culture and should be integrated into the overall risk management program rather than dealt with in isolation.

An effective FCMLTF prevention strategy and its implementation require Bank Officials to:

- Identify the areas within the business most vulnerable to the risks of FCMLTF;
- Enhance the processes already in place;
- Identify extra or alternative controls needed to reduce these risks;

- Introduce the extra or alternative controls to prevent FCMLTF in Bank-financed projects and other activities;
- Monitor the controls on an on-going basis to check that they are in operation;
- Regularly assess the effectiveness of the controls, in particular to take account of the changing circumstances in the organisation;
- Ensure that the strategy and procedures in place are workable and practical and supported by appropriate resources.

All policies, procedures and operations manuals must be regularly reviewed and updated, including in the context of a regular quality assurance by an independent third party. A control system, which may have been effective at the time of its introduction may no longer fit readily with the latest organizational structure or meet the organization's changing circumstances or needs.

Bank Officials have primary responsibility for the proper implementation of this Policy in their respective Division. It must ensure through regular control and risk self-assessments that suitable controls to prevent FCMLTF are in place, and their effectiveness must be monitored by regularly reviewing and assessing key risk indicators and qualitative factors.

All Staff Members must be regularly reminded of the importance of fostering an ethical culture and the Bank's commitment in combating FCMLTF. Education and environment play an important role for this, as does Management setting 'the tone at the top'.

As most FCMLTF experienced by an organisation is committed or tolerated by its own staff, a verification check of references and previous employment records must be made when new Staff Members is employed, following the Bank's relevant regulations. Additionally, a system of personnel management deterring Staff Members from committing or tolerating FCMLTF should be in place.

4.2.2 Importance of Know-Your-Customer Standards

Sound Know-Your-Customer (KYC) procedures have particular relevance to the safety and soundness of the Bank, in that:

- They help to protect the Bank's own reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential financial, reputational and/or other damage.

- They constitute an essential part of sound risk management, e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management.

The inadequacy or absence of KYC standards can subject the Bank to serious customer and counterparty risks, while also reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to the Bank (e.g. through the termination of inter-bank facilities, investigation costs and loan losses), as well as in the need to divert considerable management time and energy to resolving problems that arise.

Reputational risk poses a major threat, since the nature of the Bank's business requires maintaining the confidence of the shareholders, rating agencies, creditors and the general marketplace. Reputational risk is defined as the possibility that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk, because they can become a vehicle for or a victim of illegal activities perpetrated by customers, clients and financing partners. They need to protect themselves by means of continuous vigilance through an effective KYC program. Assets under management, or held on a fiduciary basis, such as private banking funds, can pose particular reputational dangers.

Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programs, ineffective control procedures and failure to practise due diligence. A public perception that the Bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the Bank.

Legal risk is the possibility that adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank.

Concern about *concentration risk* mostly applies on the assets side of the balance sheet of the Bank. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations, but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are and their relationship with other customers, it will not be possible for the Bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

The Bank's Management has important responsibilities in evaluating and ensuring adherence to KYC policies and procedures.

The Bank regularly organizes training programs for Board Officials, Bank Officials and Staff Members, so that the persons in name are adequately trained in KYC procedures. Training requirements have a different focus for new staff, front-line staff, operations staff or staff dealing with new customers. Indicatively, new Staff Members will be educated in the importance of KYC policies and the basic requirements at the bank. Front-line Staff Members, who deal directly with the public, will be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an on-going basis and to detect patterns of suspicious activity. Annual refresher training will be provided to ensure that Staff Members are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant Staff Members fully understand the need for and implement KYC policies consistently. Participation in such trainings shall be mandatory and DCR shall report to Management absences from such trainings. A culture within the Bank that promotes such understanding is the key to successful implementation.

4.2.3 Essential Elements of Know-Your-Customer Standards

4.2.3.1 Know-Your-Customer Procedures

KYC procedures for Banking operations will embrace routines for the proper management oversight, systems and controls (e.g. CDD), segregation of duties, training and other related provisions, taking also into consideration the provisions of Section 4.11 – Domiciliation of BSTDB Counterparties of this Policy. The results of the CDD, including also an assessment of and expression of an opinion on the counterparty's anti-fraud, corruption, money laundering, terrorism financing and integrity status, shall be reflected in the Bank's operations approval documents.

In respect of Treasury transactions and exposures within acceptable jurisdictions (as defined and further elaborated in the Domiciliation of BSTDB Treasury Clients rules), a CDD shall be performed for any entity, as detailed in the KYC Procedures for Treasury Counterparties, before the Bank opens a deposit and/or placement account with it (directly or through its correspondent bank) or accepts funding from it.

In consistency with FATF guidance[1], KYC procedures will follow a risk-based approach, enabling the subjecting of customers to proportionate controls and oversight.

4.2.3.2 Customer and Ultimate Beneficial Owner Identification and Verification

Before examining a transaction, the Bank should be satisfied that it has gathered information sufficient to give a view as to the identity of the ultimate beneficial owner (UBO) and how ownership is held. This is particularly relevant as concerns the identity of the borrower, but to fully protect the Bank, it may often be necessary to identify the UBOs

[1] FATF, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, High Level Principles and Procedures*, 2007 https://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf; Guidance for A Risk-Based Approach - the Banking Sector, October 2014, https://www.fatf-gafi.org/documents/riskbasedapproach/documents/risk-based-approach-banking-sector.html?hf=10&b=0&s=desc(fatf_releasedate)

of other counterparties in the transaction (sponsor, co-investor, shareholders). As a general rule, determining beneficial ownership is even more critical when equity transactions are being considered, since they entail higher risks, due to the Bank's level of involvement and the difficulty associated with exiting the relationship. KYC is not only about "who" but also "what". Where the Bank's reputational risk is linked to an individual owner(s), in particular cases of higher risk such as equity transactions or politically exposed persons (PEPs), it shall be necessary to understand the full extent of the individual's source of wealth and business dealings, in particular partners in, and activities of, the business group, to determine if there are any potential areas of risk beyond those associated with the particular transaction under consideration.

With regard to the customer and UBO identification and verification, the Bank has adopted the related recommendations of the FATF[2], the measures which the FATF Members have agreed to implement and which all countries are encouraged to adopt. These Recommendations set out the basic framework for AFCMLTF efforts and they are designed to be of universal application.

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
(b) Identifying the UBO, and verifying the identity of the UBO, to the extent that the Bank is satisfied that it knows who the UBO is. For legal persons, trusts, companies, foundations and similar legal arrangements, the Bank should take reasonable measures to understand the ownership and control structure of the customer;
(c) Assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
(d) Conducting on-going monitoring of the business relationship, including scrutiny of transactions undertaken where the Bank is a counterparty, throughout the course of the relations to ensure that the transactions being conducted are consistent with the Bank's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up to date.

When performing the measures referred to in points (a) and (b) the Bank shall also verify that any person purporting to act on behalf of the customer is so authorized and shall be required to identify and verify the identity of that person.

4.2.3.3 *Records Management*

All units should maintain, for as many years as stipulated in the Bank's relevant rules and procedures on records (currently 7 years after the business relationship is terminated), but under no condition less than the minimum period recommended by the FATF (5 years), all necessary records on transactions to enable the Bank to comply swiftly with information requests from the competent authorities of our Member States. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any).

Maintaining complete and updated records is essential for the Bank to adequately monitor its relationship with its customer, to understand the customer's on-going business and activities, and, if necessary, to provide an audit trail in the event of disputes, legal action, or inquiries or investigations that could lead to regulatory actions or criminal prosecution.

Such records comprise the CDD measures (e.g. documents and data referring to the legal status or the activity of our counterparts, banks or corporations, integrity researches, copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), operations files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions).

All personal data included in the records shall be treated in accordance with the Bank's Personal Data Protection rules.

[2] FATF, *The FATF Recommendations*, 2012, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

4.2.3.4 New Technologies

The Bank should identify and assess the money laundering or terrorist financing risks that may arise in relation to: (a) the development of new products and new business practices, including new funds transfer mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. Such a risk assessment shall take place prior to the launch of the new product, business practice or the use of new or developing technologies and appropriate measures shall be taken to manage and mitigate those risks.

4.2.3.5 Unusual Transactions

All units should pay special attention to all complex, unusual, large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help the Board of Directors and any third party the which the Bank may decide to disseminate the information.

4.2.3.6 Corporate Vehicles

The Bank should take notice of the potential for abuse of shell corporations by money launderers and should consider whether additional measures are required to prevent unlawful use of such entities. The Bank should exert every reasonable effort to understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

4.2.3.7 Introduced Business

Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate objective of the Bank to know its customers and their business. In particular, the Bank should not rely on introducers that are subject to weaker standards than those governing its own KYC procedures or that are unwilling to share copies of due diligence documentation.

If the Bank wishes to use introducers, it should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out by the Basel Committee[3]. The ultimate responsibility for knowing customers always lies with the Bank.

4.2.3.8 Correspondent Banking

Correspondent banking is: a) the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”), including but not limited to providing a current or other liability account and related services, like cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services; (b) the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly[4] (because of the lack of an international network). Large international banks typically act as correspondents for thousands of other banks around the world. Because of the structure of this activity and the limited available information regarding the nature or purposes of the underlying transactions, correspondent banks may be exposed to specific money-laundering and financing of terrorism risks (MLTF risks).

Should the Bank provide correspondent banking services to responded banks, the Bank should gather sufficient information about a respondent bank to understand fully the nature of its business and correctly assess MLTF risks on an on-going basis.

[3] Basel Committee on Banking Supervision, Sound Management of Risks related to Money Laundering and Financing of Terrorism, 2017, https://www.bis.org/bcbs/publ/d405.pdf

[4] Basel Committee on Banking Supervision, Sound Management of Risks related to Money Laundering and Financing of Terrorism, 2017, https://www.bis.org/bcbs/publ/d405.pdf

4.2.3.9 Wire Transfers

The Bank does not undertake third party payments. With regard to wire transfers for its own account, the Bank includes required and accurate originator information and required beneficiary information (including the name and the account number of the beneficiary) in wire transfers and related messages to its correspondent banks.

4.3 IDENTIFYING FRAUD, CORRUPTION MONEY LAUNDERING AND TERRORISM FINANCING

The Bank expects all its Board and Bank Officials, Staff Members, experts, consultants, contractors, counterparts and customers to be diligently on their guard for fraud, corruption, money laundering and terrorism financing and to take every reasonable measure for their prevention, deterrence and detection.

All Staff Members, irrespective of grade, position or length of service will be appropriately trained on an on-going basis, in order to be able to work towards preventing, deterring and detecting FCMLTF. FCMLTF prevention, deterrence and detection matters shall be included in the Bank's continuous career training and development activities.

4.4 PROHIBITED PRACTICES, MONEY LAUNDERING, TERRORISM FINANCING AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMD): REPORTING & INVESTIGATION

It is the responsibility of all Staff Members to stay alert for occurrences of FCMLTF and to be aware that unusual events, transactions or activities could be indications of actual or attempted FCMLTF.

Apart from the cases confronted by staff directly involved, evidence or suspicions of fraudulent, obstructive, coercive, collusive or corrupt practices (altogether called "Prohibited Practices") and of money laundering, terrorism financing or financing of the proliferation of weapons of mass destruction may also be highlighted, as a result of specific checks by Bank Officials, a third party, DCR, or in the course of audit reviews by both internal and external audit.

If there is any uncertainty as to whether an action could fall within the aforementioned practices, DCR should be contacted for guidance.

Suspicion is defined as being beyond mere speculation and based on some foundation i.e. a degree of satisfaction not necessarily amounting to a belief but at least extending beyond speculation as to whether an event has occurred or not. Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must none the less be built upon some foundation.

Whilst there is no fixed test as to what is and is not suspicious, what one can say is that anything which, is unusual in the context of the business or customer concerned, should be regarded as worthy of review and after such review, if no reasonable explanation is forthcoming, might then be deemed 'suspicious'. A 'suspicious' transaction is not necessarily one, which is definitely or even probably illegitimate. To describe a transaction as suspicious is merely to state that it merits further scrutiny.

Any suspicions of Prohibited Practices, money laundering, terrorism financing, or financing of the proliferation of WMD should be reported, if raised internally, or directed, if communicated to the Bank from external sources or through the Bank's dedicated complaints mechanism, to DCR, which, in consultation with the General Counsel, will establish the course of action for each reported suspicion. Should the suspicion be reported to DCR by means other than the Bank's complaints mechanism, DCR shall subsequently utilize such mechanism. As appropriate, DCR will establish, maintain and follow a response plan. The reported suspicion, however innocent, will be reviewed, analysed and potentially investigated as per the Bank's related procedures. If there is suspicion that a member of DCR may be involved in any of the above practices, the President and the Head of the Internal Audit Department should be informed instead. In cases of co-financing or parallel financing with other IFIs, joint investigations are explicitly allowed.

Reporting persons or entities are encouraged to submit written allegations preferably by providing his/her name, and information in as much detail as possible, including, as a minimum, what, when, where, how it happened, who committed the alleged FCMLTF, how is the allegation related to Bank's business and any corroborating evidence.

Since early reporting of suspicions facilitates more effective investigation and remediation, suspicions should be reported by the Staff Members or external parties the soonest possible after becoming aware of the suspected occurrence of such practices.

Staff Members, entities or individuals providing their name, who come forward in good faith with reasonable suspicions or evidence of occurrences of illegal, unethical or questionable practices constituting internal or external Prohibited Practices, money laundering, terrorism financing or (financing of the) proliferation of WMD (whistle-blowers) or cooperate or provide information during an ensuing review or investigation, shall be protected by the Bank from unauthorized disclosure of their identity, unless:

- they have consented to such disclosure, or
- such disclosure is necessary for proceedings under the Bank's investigations of suspected unsatisfactory conduct or misconduct and the imposition of Disciplinary Measures when reporting in bad faith, or
- the Bank has decided to accept a request by a competent judicial authority, or
- where it might impede a subject person's ability to properly answer allegations raised against them.

The Bank will exert every reasonable effort to protect such persons or entities from retaliation from Persons Connected with the Bank, as such term is defined in the Headquarters Agreement of the Bank, within the working environment or context and will treat such retaliation from the categories of Persons Connected with the Bank, being the Bank's Code of Conduct subjects, as a separate act of misconduct.

A staff member who acts maliciously, by disclosing information to DCR that he/she knows or can reasonably be expected to know to be false, shall be subject to disciplinary measures.

Anonymous reports will be accepted as a basis for a review/analysis/investigation. However, DCR's capacity to follow up such reports may be limited.

If it will be deemed that there is serious evidence of FCMLTF committed by a correspondent bank, supplier, consultant or customer, then the issue will be reported -through the Bank's Management Committee- to the Board of Directors of the Bank, which in turn will decide about reporting it to the competent Financial Intelligence Unit (FIU) or any other competent authority (-ies). Every Member State will be requested to provide information about its domestic competent authorities in relation thereto.

If borrowing financial institutions, or other businesses or entities transacting with the Bank, suspect or have reasonable grounds to suspect that funds with which they are somehow involved are linked to money laundering activities, or are linked to, related to, or are to be used for terrorist acts or by terrorist organizations, they should be required to report promptly their suspicions to their competent authorities and notify the Bank accordingly.

Board and Bank Officials and Staff Members are not allowed to warn in any way, any of the suspected parties or anyone else associated with them when information relating to them is being reported to the DCR, Internal Audit Department, the Bank's President, the Board of Directors or the competent authorities, comprising the authorities of the Bank's Member States and international organizations such as Interpol.

4.5 ABOUT FRAUD AND CORRUPTION

4.5.1 What is fraud?

A business or organization may be exposed to:

- external fraud, perpetrated by individuals outside the organization;
- internal fraud, perpetrated by management or employees;
- coercion, perpetrated by individuals inside or outside the organization;
- collusion, between individuals inside or outside the organization.

Fraud encompasses an array of irregularities and illegal acts characterized by intentional deception.

There is no precise, universal, legal definition of fraud and no single criminal offence that can be called fraud. It is usually but not necessarily taken to involve theft or defalcation -the removal of cash and assets to which the

fraudster is not entitled-, improper and unlawful enrichment, improper use of assets and other items, false accounting -falsification or alteration of accounting records or other documents- and other fiscal irregularities. According to the International Federation of Accountants[5], "fraud is an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage" and "fraud risk factors are events or conditions that indicate an incentive or pressure to perpetrate fraud, provide an opportunity to commit fraud, or indicate attitudes or rationalizations to justify a fraudulent action."

According to the International Financial Institutions Anti-Corruption Task Force[6] and the World Bank[7]:

- A **fraudulent practice** is any action or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation.

- A **coercive practice** is impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to influence improperly the actions of a party.

- A **collusive practice** is an arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party.

- An **obstructive practice** is a) deliberately destroying, falsifying, altering or concealing of evidence material to the investigation or making false statements to investigators in order to materially impede a Bank investigation into allegations of a corrupt, fraudulent, coercive, or collusive practice; and/or threatening, harassing, or intimidating any party to prevent it from disclosing its knowledge of matters relevant to the investigation or from pursuing the investigation, and b) acts intended to materially impede the exercise of the Bank's investigation and audit rights to contractually required information in connection with an allegations of a corrupt, fraudulent, coercive or collusive practice.

Although the management of risk is one of the most important issues facing financial institutions, fraud has always been a serious threat to their financial health and to their image and reputation.

While the threat of fraud has always existed, the opportunities for it may now be expanding due to:

- An increasingly sophisticated workforce and the expanded use of Information Technology (IT), which creates new opportunities for fraud.
- Desk-top publishing that makes it is easier to produce dummy invoices, bank statements and other third-party documents.
- The use of external consultants or total outsourcing of key functions in areas such as IT, accounting, contract tendering, and other professional services.

4.5.2 Common Frauds

Generally, fraud may be divided into two main types:

Profit and loss frauds:
An organization is likely to be vulnerable to a variety of small frauds. These may be difficult to detect as individually they may be for relatively small amounts (though over time they may be significant). Large frauds would be likely to be discovered; however, whether this is in time to save the business is uncertain. Therefore, in terms of impact, the amount of time taken to spot a fraud is key.

[5] International Federation of Accountants, *International Standard on Auditing 240*, http://www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf

[6] *Uniform Framework for Preventing and Combating Fraud and Corruption*, 2006
[7] World Bank, *Procurement Guidelines and the Guidelines for Selection and Employment of Consultants*, 2014
http://pubdocs.worldbank.org/en/894361459190142673/ProcurementConsultantHiringGuidelinesEngJuly2014.pdf

Balance sheet frauds (i.e. cut-off problems, accounting data manipulation, etc.):
These often tend to increase in size, thus, leading to discovery, even though such frauds may not necessarily involve misstated financial reports.

Whilst the risk of fraud may be greatest in those businesses handling cash or consumer goods, it is widely accepted that all businesses are vulnerable to fraud of one sort or another.

The risk due to fraud may come from four broad categories (the examples mentioned in each category are not exhaustive):

a. Employees abusing their position or making misrepresentations:
- The misappropriation of assets (such as cash, stock, reimbursement of expenses, payroll, stationery, etc.);
- Malicious destruction of assets;
- Transactions not reported intentionally;
- Unauthorized transaction;
- Mismarking of position intentionally;
- The manipulation of documents – this can include altering documents as well as producing false ones;
- Theft of confidential information or of intellectual property;
- Bonus-based frauds – managers may manipulate information on which their bonuses or performance appraisals may be based;
- Profiteering as a result of insider knowledge of securities or financing activities, or disclosing to other persons the securities or financing activities engaged in, or contemplated by the Bank;
- Employees extracting benefits they are not entitled to.

b. Suppliers taking advantage of their customers (the latter being either the Bank itself or its borrowing customers):
- A supplier of goods or services may recognize weak or non-existent checking controls. This can result in fewer items being delivered than stated on the delivery note, or even the wrong type of goods. Without sufficient checks on goods received it may be difficult to complain later. Another common fraud is to invoice for the wrong quantity or at the wrong price.
- The company purchaser(s) may not be independent (e.g. he/she may be related to, or be receiving advantages from the supplier). This can result in substandard goods being bought at an uncompetitive price. This fraud is an example of corrupt practices by employees and is dealt in more detail in the Section under Corruption (below).
- Directory fraud is whereby fictitious invoices or letters are received. Unless the business has an authorization process to identify fictitious invoices, there is a danger that the recipient will pay simply because their company's name is on the invoice.
- Maintenance or subscription costs – fees may be taken, but the supplier may not provide a proper service

c. Customer frauds:
- The most frequent and significant type of fraud performed against banking institutions by customers or potential customers is various techniques to by-pass due diligence controls in order to obtain credit that will not be repaid or used as agreed.
- More significant frauds may occur if employees collude with either suppliers or customers.

d. Information Technology Fraud:
- A threat to an organization's security can come about when upgrading or replacing a computer system. An unscrupulous consultant/retailer may be able to fraudulently alter data or access confidential files.
- Another possible source of threat may come from the internet, e.g. hacking, which is circumventing or bypassing the security mechanisms of an information system or network for destroying, disrupting or carrying out illegal activities on the network or computer systems.
- New technological developments may present a whole new range of threats, e.g. the improper use of the e-mail system.

Tax fraud - tax evasion versus tax avoidance or mitigation:

It is often difficult to assess with certainty and distinguish between illegal "tax evasion" from legal "tax mitigation or avoidance", due to the complexity of the tax schemes, the ambiguities in some tax laws, as well as due to erratic

enforcement by tax authorities. This is exacerbated by the fact that, in some countries, allegations of illegal tax practices and the instigation of tax investigations are often misused to discredit competitors or to damage political enemies. The main causes of avoidance and evasion are high taxes, imprecise laws, insufficient penalties and lack of equity in the tax system.

However, the “business purpose” test aimed at determining whether there is an underlying legitimate purpose to the transaction is found in many states’ tax laws and may provide some guidance. The “business purpose" test breaks down the transaction into its component steps to determine the true purpose of the transaction(s). If the transaction has no commercial purpose other than the avoidance of tax, then it constitutes tax evasion (illegal). If the transaction has a commercial purpose, then the resulting tax avoidance may be deemed legal. Outside legal advice should be sought to interpret local law and prevailing business practices, including the relevance or applicability of the business purpose test.

In order to avoid the reputational risk of becoming associated with potentially illegal tax activities, the Bank must be able to accurately assess any related risk and to take measures commensurate with that risk.

Tax Evasion

Tax evasion, in general, refers to illegal and fraudulent actions which lead to escape from taxation. In other words, tax evasion can be defined as **the deliberate effort by companies, institutions, organizations, individuals and other entities to evade tax by illegal methods.** This illegal activity can be operated by a false declaration or no declaration at all of taxes due to the relevant tax authorities, or by the deliberate misrepresentation or conceal of the true state of affairs by destroying or fabricating records, keeping parallel accounts, failing to report income, or smuggling. Tax evasion is a crime.

Tax avoidance

Tax avoidance, on the other hand, encompasses the use **of legal activities, in order for the taxpayer to avoid paying taxes or reduce the tax liabilities,** by implementing methods that take advantage of the tax code and exploit the loopholes of the relative legislation. The practice of tax avoidance takes place at these sections and areas of the tax code which are ambiguous and in need of further interpretation. The most important difference between tax evasion and tax avoidance is that the former is related to illegal activities, whereas tax avoidance succeeds in minimizing tax liabilities by actions that are in accordance to the tax law.

4.5.3 What is corruption?

Corruption is a term associated with various illegal or immoral activities or behaviours. In the context of banking and International Financial Institutions, corruption may best be defined as the abuse of official -public or private- office or position for personal gain or enrichment, or the misuse of one’s position to assist others in improperly or unlawfully enriching or empowering themselves.

4.5.4 Causes of Corruption

Corruption within an organization arises due to various factors, including:

- The lack of an effective ethical and control awareness culture;
- Ineffective corporate governance, policies, procedures and internal controls;
- Inappropriate, ambiguous and/or overly complicated rules and procedures offering large and unclear scope for interpretation, with little oversight;
- Lack of transparency and inadequate communication channels;
- Low wages of staff, limited job satisfaction or an unfair remuneration/ benefits system, perceptions of unfair treatment.

With regard to the public sector, causes of corruption may be rooted in a country's policies, bureaucratic traditions, political development, and social history. Corruption tends to flourish, when institutions are weak and government policies generate rents[8]. The dynamics of corruption can be depicted in a simple model suggested by Klitgaard (1998):

C=M+D-A

where: C (corruption) = M (monopoly) + D (discretion) - A (accountability)

This model suggests that corruption will tend to emerge when an organization or person has monopoly power over a good or service which generates rent, has the discretion to decide who will receive it (thus on how rents will be allocated), and is not accountable.

4.5.5 Corrupt Practices

According to the International Financial Institutions Anti-Corruption Task Force[9], a corrupt practice is the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.

According to OECD[10], "Bribery is a specific form of corruption that can be defined as the voluntary giving of something of value to influence performance of official duty either by doing something improper or failing to do something they should do within the authority of their position."

Corrupt practices and consequently the efforts to combat corruption may broadly rest upon the following three pillars (with illustrative examples -non exhaustive- of corrupt behaviours):

a. Corruption at the micro-level (or "individual corruption") - such as corrupt practices within the governance of the organization and Bank-financed projects:

- The design, selection or tolerating of uneconomical projects because of opportunities for financial kickbacks and political patronage.
- Procurement fraud, including collusion, overcharging, or the selection of contractors, suppliers, and consultants on criteria other than the lowest evaluated substantially responsive bidder.
- The misappropriation of confidential information for personal gain.
- The deliberate disclosure of false or misleading information on the financial status of corporations that would prevent potential investors from accurately valuing their worth, such as the failure to disclose large contingent liabilities or the undervaluing of assets in enterprises slated for privatization.
- The sale of official posts, positions, or promotions; nepotism; or other actions that undermine the creation of a professional, meritocratic service.
- Extortion and the abuse of office, such as using the threat of a performance appraisal or disciplinary sanctions to extract personal favours.
- The acceptance of gifts in excess of a customary or insignificant amount, whether financial or non-financial, which may influence the actions of a Bank's employee.

b. Corruption at governmental or country level (or "systemic corruption"):

- Illicit payments of "speed money" to government officials to facilitate the timely delivery of goods and services to which the public is rightfully entitled, such as permits and licenses.
- Illicit payments to government officials to facilitate access to goods, services, and/or information to which the public is not entitled, or to deny the public access to goods and services to which it is legally entitled.
- Illicit payments to prevent the application of rules and regulations in a fair and consistent manner, particularly in areas concerning public safety, law enforcement, or revenue collection.
-

[8] Rent is the extra amount paid (over what would be paid for the best alternative use) to somebody or for something useful whose supply is limited either by nature or through human ingenuity. Paolo Mauro, *Why Worry About Corruption?*, 1997, IMF Economic Issues, https://www.imf.org/external/pubs/ft/issues6/issue6.pdf

[9] *Uniform Framework for Preventing and Combating Fraud and Corruption*, 2006

[10] OECD, *Bribery Awareness Handbook for Tax Examiners*, 2009, https://www.oecd.org/tax/crime/37131825.pdf

- Payments to government officials to foster or sustain monopolistic or oligopolistic access to markets in the absence of a compelling economic rationale for such restrictions.
- The theft or embezzlement of public property and monies.
- Obstruction of justice and interference in the duties of agencies tasked with detecting, investigating, and prosecuting illicit behaviour.

c. Organized corruption at an international level:

- "Syndicated corruption" encompasses elaborated systems that are devised for receiving and disseminating bribes, often internationally, whilst "non-syndicated corruption" involves individual officials that may seek or compete for bribes in an ad hoc and uncoordinated fashion.

Apart from the courtesy gift items (corporate gifts and protocol presents) or reasonable travel and accommodation expenses for approved events and representations, the Bank does not, directly or indirectly, offer, promise or give any advantage to public officials or the employees of business partners. Likewise, the Bank does not request, agree to or accept any pecuniary or other advantage from public officials or the employees of business partners.

4.5.6 Politically Exposed Persons (PEPs)

Business relationships with individuals who held or are currently holding important public positions, their immediate family members and persons known to be their close associates, or with companies clearly related to these individuals in their capacity as Executive Directors, members of the Management Committee or UBOs, may expose a bank to significant reputational and/or legal risks. There is always a possibility that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.; such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the Bank may be subject to costly information requests or other requests.

Any business relationship of the Bank involving interests of a PEP who otherwise has a direct relationship with the Bank (i.e. a person connected with the Bank), and which interests are not prohibited by the Bank's Code of Conduct, requires specific approval by the Bank's Board of Directors.

Finally, Management's approval for establishing business relationships with such customers shall be obtained (at the appropriate committee level, be it Credit Committee, Management Committee or equivalent).

4.6 ABOUT MONEY LAUNDERING

4.6.1 What is money laundering?

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source.

Such criminal acts can generate huge sums and create the incentive to "legitimize" the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

According to a widely accepted definition[11], "money laundering" includes the following:

-

[11] Directive 2015/849 of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, consistent with the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) [*"Vienna Convention"*], the United Nations Convention against Transnational Organized Crime (2000) {*"Palermo Convention"],* and the United Nations Office of Drugs and Crime and IMF*, Model Legislation on Money Laundering and Financing of Terrorism,* 2005*,* https://www.unodc.org/documents/money-laundering/2005%20UNODC%20and%20IMF%20Model%20Legislation.pdf

- the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;
- the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
- participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing indents.

Knowledge, intent or purpose required as an element of the above activities may be inferred from objective factual circumstances.

Money launderers are continuously looking for new routes for laundering their funds. Economies with growing or developing financial centres, but inadequate controls, are particularly vulnerable, as established financial centre countries implement comprehensive anti-money laundering regimes.

4.6.2 How is money laundered?

In the initial or placement stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

After the funds have entered the financial system, the second –or layering– stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

Having successfully processed his criminal profits through the first two phases of the money laundering process, the launderer then moves them to the third stage –integration– in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

The risk for the Bank lies in its potential engagement in: i) financing projects used as vehicles to launder money earned from criminal activities, or ii) financing or engaging in business transactions with banks that could be involved in money laundering or banks that do not take all necessary measures to avoid financing customers involved in money laundering. Maintaining the Bank's good reputation is of paramount importance.

4.7 ABOUT TERRORISM FINANCING

4.7.1 What is terrorism financing?

According to a widely accepted definition[12] "terrorist financing" means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the following offences:

[12] Directive 2015/849 of the European Parliament and of the Council on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing, consistent with the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) ["*Vienna Convention*"], the United Nations Convention against Transnational Organized Crime (2000) {"*Palermo Convention"],* and the United Nations Office of Drugs and Crime and IMF, *Model Legislation on Money Laundering and Financing of Terrorism*, 2005, https://www.unodc.org/documents/money-laundering/2005%20UNODC%20and%20IMF%20Model%20Legislation.pdf

a. attacks upon a person's life which may cause death;

b. attacks upon the physical integrity of a person;

c. kidnapping or hostage taking;

d. causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major political and/or economic disruption and major economic loss;

e. seizure of aircraft, ships or other means of public or goods transport;

f. manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of biological and chemical weapons;

g. release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life;

h. interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life;

i. threatening to commit any of the acts listed in a. to h.;

j. public provocation to commit terrorist offences;

k. recruitment for terrorism;

l. training for terrorism;

m. aggravated theft with a view to committing one of the offences listed from a. to h;

n. extortion with a view to the perpetration of one of the offences listed from a. to h;

o. drawing up false administrative documents with a view to committing one of the offences listed from a. to h. and participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Knowledge, intent or purpose required as an element of the above activities may be inferred from objective factual circumstances.

These intentional acts, defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, shall be deemed to be terrorist offences where committed with the aim of:

- seriously intimidating a population, or
- unduly compelling a Government or international organization to perform or abstain from performing any act, or
- seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

In examining the financing of terrorism, it is important to distinguish two types: i) financing of terrorism through money laundering and ii) financing of terrorism through the use of legitimate funds. If the criminal proceeds of a predicate offense were used to finance terrorism, this would constitute both money laundering and financing of terrorism and would be caught by the provisions of most national anti-money laundering laws.

The second type of financing of terrorism involves the use or abuse of legitimate funds to finance terrorism.

Respective examples:
(1) Proceeds of crime (*e.g.,* from drug trafficking) are laundered and used to finance acts of terrorism.
(2) Legitimate funds like donations made to charities or foundations are diverted to finance acts of terrorism.

4.7.2 The Link between Money Laundering and Terrorism Financing

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorism financing. Funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorism financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorism financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

4.7.3 Combating Financing of Terrorism

Given that both money laundering and financing of terrorism are typically committed through the abuse of financial institutions, thereby undermining financial sector governance, and that there are some common approaches and measures to prevent, detect, and counter them, the fight against MLTF calls for the adoption of a consolidated strategy and approach. Several international, regional, and specialized bodies, among others the FATF, the United Nations, the International Monetary Fund (IMF), the World Bank and FATF-style regional bodies have in close collaboration developed a number of strategies and instruments depending on their respective mandates.

The number and seriousness of acts of international terrorism depend on the financing that terrorists may obtain. In that frame Financial Institutions have been called to take appropriate measures, thus becoming partners in a strategic combat.

Such measures also include compliance with the sanctions set by the United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing that require ensuring that no funds and other assets are made available to or for the benefit of any natural or legal person or entity designated by the United Nations Security Council resolutions imposing targeted sanctions in the terrorist financing context.

4.8 ABOUT FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (WMD)

"Financing of proliferation of weapons of mass destruction (WMD)" refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.[13]

Proliferation differs from money laundering in several respects. The fact that proliferators may derive funds from both criminal activity and/or legitimately sourced funds means that transactions related to proliferation financing may not exhibit the same characteristics as conventional money laundering. Furthermore, the number of customers or transactions related to proliferation activities is likely to be markedly smaller than those involved in other types of criminal activity such as money-laundering[14].

In most jurisdictions, robust systems are likely in place aimed at the prevention and detection of this procurement activity related to development of prohibited programs or capabilities, particularly through the imposition of export controls on proliferation of sensitive goods, technology, knowledge and services, as well as secret and criminal intelligence efforts aimed at identifying, investigating, disrupting and taking action to disrupt proliferation networks. Efforts to combat the financing of proliferation of WMD must therefore be integrated into these established structures[15].

---

[13] The working definition developed by FATF as set out in: FATF, *Combating Proliferation Financing: a Status Report on Policy Development and Consultation*, 2010, https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf

[14] FATF, *Combating Proliferation Financing: a Status Report on Policy Development and Consultation*, 2010, https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf

[15] FATF, *Best Practices Paper to Recommendation 2: Sharing among Domestic Competent Authorities Information related to the Financing of Proliferation*, 2012, **http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20on%20Recommendation%202%20Sharing%20among%20domestic%20competent%20authorities%20re%20financing%20of%20proliferation.pdf**

According to FATF[16], related measures include compliance with United Nations Security Council resolutions[17] that require, inter alia, ensuring that no funds and other assets are made available, directly or indirectly to or for the benefit of, any natural or legal person or entity designated by the United Nations Security Council under Chapter VII of the Charter of the United Nations, pursuant to Security Council resolutions that relate to the prevention and disruption of the financing of proliferation of weapons of mass destruction. The Bank's KYC Procedures shall include checking of such compliance.

As per the Bank's Exclusion List, the Bank does not finance, inter alia, operations that directly or indirectly involve production, use, distribution, business or trade of weapons, ammunition, military goods or goods that may be directly used for military purposes, and transactions which contravene any applicable laws or international conventions in all relevant jurisdictions, or United Nations Security Council sanctions.

4.9 QUANTITATIVE DATA MONITORING

DCR shall monitor FCMLTF and KYC-related quantitative data in a practicable manner, so as to report it to the Management and to the Audit Committee, as appropriate.

4.10 ROLE of DCR

DCR, being responsible for the overall ownership of the Bank's AMLCTF program and efforts, shall have the responsibility to prepare appropriate KYC Procedures.

DCR shall provide guidance and consultancy to the operation teams on KYC and integrity-related/KYC issues, mainly during the Customer Due Diligence (CDD) and Supervision and Monitoring stages of an operation, as per the KYC Procedures, and upon request assist the Information Unit (IU) and Credit/Management Committee with integrity-related/KYC issues.

DCR shall report to the President on a regular basis and upon a relevant request report any issues to the Audit Committee of the Bank's Board of Directors.

DCR shall oversee that all persons within the scope of the present Policy are trained on how to prevent AMLCTF.

The application and effectiveness of the present Policy shall be reviewed periodically by DCR, taking into account the international best practices in the prevention and combat of AMLCTF, as well as experience acquired through the implementation of the Policy and market practices on the subject, in order to update it, as required.

Compliance with the present Policy shall also be reviewed periodically by DCR.

4.11 DOMICILIATION OF BSTDB COUNTERPARTIES

Preamble:

As an international financial institution with a mandate to effectively contribute to the transition process of the Member States towards the economic prosperity of the people of the region, and to finance and promote regional projects and provide other banking services to projects of the public and private sectors in the Member States and trade activities among the Member States, the Bank supports international efforts to combat AML/CTF and discourage tax evasion and other harmful tax practices. In its own operations, the Bank supports the principle of taxation of economic activity in accordance with tax laws and international tax treaties. In this context it is important that local tax authorities have access to the relevant information to monitor compliance with these laws and treaties. This may become more difficult when jurisdictions other than the one where the project is located are chosen as locations for establishment of intermediary or controlling entities involved in the Bank operations. Therefore, when such jurisdictions are used, the Bank makes use of internationally agreed

[16] FATF, *The FATF Recommendations 2012*, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf - Recommendation 7

[17] At the time of issuance of Recommendation 7 (February 2012), the United Nations Security Council resolutions applying targeted sanctions relating to the financing of proliferation of weapons of mass destruction were: 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010).

processes and best practices designed to prevent misuse and to promote transparency and information exchange on tax matters.

As mandated by Section 2.c of the Procedure for Financing Projects and Commercial Activities, the "Bank shall be guided by sound banking principles and by considerations of transparency and accountability in all its operations". One such principle is the KYC, which requires that the Bank conduct appropriate due diligence on operations sponsors and the operations themselves. In each case, the corporate governance structure, beneficial ownership, financial transparency and strength, compliance and integrity, including in relation to tax matters, are reviewed according to best practices. Naturally, similar assessments are also made in operations involving intermediate vehicles established in a jurisdiction different from the one where the project is located, with a view, among others, to obtaining a reasonable level of assurance that the intermediate structure is not set up or used for the purpose of tax evasion, money laundering and terrorism financing.

With its project finance and private sector focus, the Bank has had to deal with intermediate vehicles since its inception. This is because the use of such vehicles is not uncommon practice for private sector investors in international project finance and when engaged in cross- border investment. Where jurisdictions other than the one where the operation is located are used, the Bank's long-standing practice has also been to satisfy itself that the reasons for using such structures are sound from a business viewpoint. Sound business reasons may include the need to establish a common investment vehicle in a stable and/or investor-friendly jurisdiction. The choice of other jurisdictions may be influenced by the desire to avoid double taxation, as legally permitted by a network of bilateral treaties and national tax laws.

Where such structures are used, the Bank's practice has been to assess whether or not there is a risk that the jurisdictions are associated with improper financial activities. This chapter respects and builds on these objectives and underscores the role of the Bank in supporting international efforts to combat such activities, in particular by making use of the peer group assessments of the Global Forum as well as the work of the FATF in countering money laundering and terrorism financing risks.

Prospective clients presenting to the Bank financing proposals that involve such structures may be adversely affected by the operation of the policy, where e.g. involved jurisdictions are poorly rated by the Global Forum. Accordingly, where needed, Management will actively manage its pipeline of operations including by directing the attention of clients to the published findings and overall ratings of the Global Forum and by stressing the risks associated with the jurisdictions not achieving a better rating ahead of the Board consideration of the proposal.

Furthermore, it has become clear that similar policy considerations are present in Bank transactions with Treasury counterparties. Therefore, in Section 4.11.8 below, the *mutatis mutandis* guidelines for the appropriate extension of the principles and objectives of this policy to Treasury operations have been included.

Ordinarily the Bank lends to, invests in, or guarantees obligations of, a "**project entity**" established in the Member State where the operation so financed is located. In some cases, however, the borrower, investee or guaranteed entity will be an "**intermediate entity**" established in a Member State different from the Member State where the operation is located, or in a "**third jurisdiction**", i.e., a country or territory different from a Member State.

In addition, a borrower, investee or guaranteed entity, wherever located, may be controlled by an entity, which "**controlling entity**" is established either in a Member State or in a third jurisdiction. "Control" for this purpose means the power of an entity to govern the financial and operational policies/aspects of the entity of which it is a shareholder. **Control** is meant as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of another person.

4.11.1 Sound business reasons

Whenever an operation considered by the Bank involves an intermediate entity or a controlling entity established in a third jurisdiction or in a Member State different from the Member State where the operation is located, as well as in the special case of the second sentence of Section 4.11.8 below, the Bank shall satisfy itself that there are **sound business reasons** for the selection and use of such third jurisdiction, Member State, or Issuer's jurisdiction.

a. Whether there are sound business reasons in a given project will depend on the surrounding circumstances. Such reasons might include (i) the desire to use a jurisdiction to attract capital from multiple sources, (ii) the need to consolidate assets across multiple jurisdictions, (iii) access to an investment protection treaty, (iv) the existence of stable legal systems which facilitate contract enforcement and registration of security, (v) the existence of clear laws regarding issues such as governance, liability and taxation, and (vi) recognition of internationally accepted investment agreements, including shareholder agreements and put options, corporate forms that ensure limited liability of shareholders, and instruments such as preferred shares.

b. The use of a third jurisdiction may involve tax planning using lawful practices and double taxation treaties, provided that (i) there are sound business reasons for the use of that third jurisdiction, (ii) such tax planning does not involve the elimination or near elimination of taxation deriving from **arrangements or methods inconsistent with the declarations, recommendations or international standards agreed by the OECD or the G20 regarding** harmful tax practices, which are duly considered.

Except in the case of repeat or follow-on projects with the same client where a questionnaire has already been used (and remains up-to-date) and the Control structure has remained substantially unchanged, the Bank shall assess the reasons for the use of a third jurisdiction and the tax implications thereof on the basis of detailed replies from the client, supplied in response to the relevant Bank's questionnaire.

The questionnaire referred to in the previous paragraph shall be designed to facilitate the assessment of compliance with Section 4.11.1 b.

4.11.2 Principles regarding the fight against money laundering and terrorism financing

In accordance with its mandate to effectively contribute to the transition process of the Member States towards the economic prosperity of the people of the region, the Bank provides financing with respect to projects located in such countries, including projects that may involve intermediary or controlling entities established in a third jurisdiction. Nonetheless,

a. where (x) a Member State, or (y) a third jurisdiction in which any intermediate or controlling entity involved in a prospective project of the Bank is established, is a jurisdiction in respect of which the FATF has released a public statement formally calling for specified counter-measures by its members and others i) the Board shall, promptly after any such public statement has been released, and based on a report from Management, review the situation arising out of the FATF's call and determine what appropriate action (including actions identified by the FATF as examples of counter-measures that could be undertaken), consistent with the Agreement Establishing the Bank, should be taken by the Bank in respect of that jurisdiction, in the case of (x) above; and ii) the Bank shall not provide financing in the case of (y) above.

b. where (x) a Member State, or (y) a third jurisdiction in which any intermediate or controlling entity involved in a prospective project of the Bank is established, is a jurisdiction in respect of which the FATF has released a public statement formally calling its members to consider the risks arising from the deficiencies associated with that jurisdiction, any operation that involves a project entity, an intermediate entity or a controlling entity established in that jurisdiction shall undergo enhanced due diligence, in order to satisfy the Bank that the entities established in that jurisdiction are not being used as vehicles for money- laundering or terrorism financing.

c. Where (x) a Member State, or (y) a third jurisdiction in which any intermediate or controlling entity involved in a prospective project of the Bank is established, is a jurisdiction in respect of which the FATF has released a public document identifying jurisdictions with strategic AML/CFT deficiencies that have developed an action plan with the FATF and provided a written high-level political commitment to address the identified deficiencies, any operation that involves a project entity, an intermediate entity or a controlling entity established in that jurisdiction shall undergo usual or enhanced due diligence, as may be deemed appropriate by Management.

4.11.3 Principles regarding effective implementation of the tax standard

An operation considered by the Bank may involve an intermediate entity, or a controlling entity established in a third jurisdiction (subject to the special case of Section 4.11.7 below).

If the third jurisdiction is a jurisdiction which is not effectively implementing the internationally agreed standards on Tax Transparency, determined by reference as more specifically described in the following paragraph, the Bank shall not provide financing.

Whether a third jurisdiction is or is not effectively implementing the internationally agreed standards on Tax Transparency is to be determined by reference to the work of the Peer Review Process of the Global Forum. More particularly,

a) a third jurisdiction for which an overall rating of "compliant" or "largely compliant" or "provisionally largely compliant" has been issued by the Global Forum shall be deemed to be effectively implementing the internationally agreed standards on Tax Transparency, unless that third jurisdiction has been identified as "non-cooperative" by the OECD or the G20.

b) a third jurisdiction for which an overall rating of "partially compliant" or "provisionally partially compliant" or "non-compliant" has been issued by the Global Forum shall be deemed not to be effectively implementing the internationally agreed standards on Tax Transparency.

c) a third jurisdiction will be deemed to meet international norms until the results of the Peer Review Process indicate otherwise. Thus, jurisdictions for which an overall rating by the Global Forum has not been assigned, shall be deemed to be effectively implementing their commitment to the internationally agreed tax standard.

4.11.4 Suspension of Section 4.11.3 b.

For any third jurisdiction to which Section 4.11.3 b) applies:

a) Unless the Board of Directors decides otherwise, the operation of that Section shall be suspended for a period of fourteen months starting from the date of the publication of the overall rating of the Global Forum, provided that such jurisdiction has made, no later than three months after the date of such publication, **a commitment to correct the deficiencies identified in the report of the Global Forum**. Such commitment shall be evidenced by a public expression of intent to execute concrete plans for legislative or other governmental and/or administrative action to address any such deficiencies **within a reasonable timeframe**. Such commitment will be communicated to the Board of Directors.

If the jurisdiction has not made such commitment within three months after the date of the publication of the overall rating of the Global Forum, such suspension period will come to an end.

b) If, within the suspension period referred to in a) the third jurisdiction has filed a request for a supplementary review and the Global Forum's peer review group has determined that such a review is warranted, the suspension period will be extended until the date when the draft supplementary report approved by the Global Forum's peer review group is submitted to Global Forum's members and observers.

If, within the suspension period referred to in a), the third jurisdiction has not filed a request for a supplementary review with the Global Forum or the Global Forum's peer review group has not determined that such a review is warranted, such suspension period will come to an end.

c) If a draft supplementary review has been approved by the Global Forum's peer review group and submitted to Global Forum's members and observers, and if such review concludes that the third jurisdiction should be assigned a revised overall rating of "largely compliant" or "compliant", the suspension period referred to in b) will be extended until the publication of the overall rating as adopted by the Global Forum.

If such review concludes that the third jurisdiction should not be assigned a revised overall rating of "largely compliant" or "compliant", such suspension period will come to an end.

d) Whenever a project considered by the Bank involves an intermediate or a Controlling Entity established in a third jurisdiction in respect of which a suspension period applies in accordance with this Section 4.11.4, the Bank shall satisfy itself that the use of the third jurisdiction is not related to the deficiencies identified by the Global Forum.

4.11.5 Exemption where controlling entity is established in its home jurisdiction

The beneficiary of a Bank's loan, equity investment and/or guarantee may be an entity established in the Member State where the operation is located while the controlling entity is established in a third jurisdiction or a Member State different than the Member State where the operation is located. Such is the case, for instance, when a foreign strategic investor has acquired or – concurrently with the Bank's operation – is acquiring a majority interest in the project entity.

The controlling entity is considered to be established in its home jurisdiction, in which case such situations shall not be reviewed under Sections 4.11.1 and 4.11.3 of this policy, if the controlling entity is established

a. in the same jurisdiction as the entities or individuals who ultimately control it, or

b. in the jurisdiction where its capital stock, or the entity's that ultimately Controls the beneficiary of a Bank's loan, equity investment and/or guarantee, has its primary listing.

If, however, the controlling entity chooses to invest through an intermediate entity established in a jurisdiction different from its home jurisdiction, then the situation must be reviewed under this policy. Likewise, where the controlling entity is itself controlled by entities and individuals established in a different jurisdiction, the situation shall be reviewed under Sections 4.11.1 and 4.11.3 of this policy.

For the avoidance of doubt, where the controlling entity's home jurisdiction appears on a public statement or document released by the FATF, the situation shall be reviewed under Section 4.11.2 of this policy.

Notwithstanding the above, Sections 4.11.1 and 4.11.3 shall apply if the Bank's integrity due diligence has indicated that the use of the third jurisdiction concerned is suspicious.

4.11.6 Exemption in case of relocation of affected entity

Notwithstanding Section 4.11.2 and 4.11.3, the Bank may provide financing where, as a condition of providing such financing, it secures a contractual undertaking (the breach of which would entitle the Bank to exercise legal remedies) to relocate the intermediate or controlling entity to another jurisdiction before first disbursement. The choice of such other jurisdiction should be consistent with the principles set out in Section 4.11.2 and 4.11.3.

4.11.7. Information of the Board of Directors/ALCO

a. Where Section 4.11.2 b applies, the Board/ALCO document shall confirm that the project underwent enhanced due diligence and shall set out the outcome of such EDD. DCR opinion shall have been incorporated.

b. Where Section 4.11.2 c applies, the Board/ALCO document shall confirm that the project underwent usual or enhanced due diligence as was deemed appropriate by Management and shall set out the outcome of such EDD. DCR opinion shall have been incorporated.

c. Where Section 4.11.4 applies, the Board/ALCO document shall confirm that the conditions set forth in such Section are met.

d. Where Sections 4.11.1 b applies, the Board/ALCO document shall set out the sound business reasons, such as those referred to in Section 4.11.1, for the selection and use of such third jurisdiction or Member State. Except in the case of repeat or follow-on projects with the same client, the information will be based on detailed replies from the client, including supporting documents, supplied in response to relevant questions prepared by Management in order to determine the existence of sound business reasons.

e. Where any of Sections 4.11.2 (AMLCTF) or 4.11.3 (tax standard) or 4.11.6 (relocation) apply, the Board/ALCO document shall confirm that the relevant jurisdiction is acceptable under the respective Section or, that there is a contractual undertaking to change the place of incorporation of the relevant entity within a specified time from signing of the principal financing documents.

f. Where Section 4.11.5 (home) applies, the Board/ALCO document shall provide any information necessary to substantiate such a conclusion.

g. Where, in accordance with Section 4.11.6 (relocation), the Bank has required, as a condition of providing financing, a contractual undertaking to change the place of incorporation of the entity within a specified time from the signing of the principal financing documents, the Board/ALCO document shall also provide information about such contractual undertaking and the reasons for requiring it, specifying the jurisdiction where the new or transferred entity will be located.

h. Guiding forms for the provision of the above relevant/respective information to Board/ALCO, as per the operation's particularities, will be available in a special section in the Bank's intranet under "Code of Rules". These Board-approved forms accompany and supplement this policy.

4.11.8 Extension of the principles and objectives of the present policy to the Bank's Treasury operations

Section 4.11.2 (FATF) above shall apply mutatis mutandis whenever there are the respective FATF releases described in such section for a jurisdiction in which an intended Treasury counterparty or its controlling entity in a prospective operation of the Treasury of any type is established. Section 4.11.3 (tax standard) above shall apply mutatis mutandis only in cases where (a) the Treasury operation is a purchase of any securities from an issuer who (b) is domiciled in a third jurisdiction (the "issuer's jurisdiction") that is different from the one in which the principal economic activity being funded by such securities is located.

4.11.9 Miscellaneous provisions

This chapter shall be reviewed as and when appropriate, in particular when international efforts to combat tax evasion, money laundering and terrorism financing have progressed to a stage where material changes to the Chapter can be reasonably envisaged in light of significant developments at the international level.

5 References

1. Basel Committee on Banking Supervision, *Sound Management of Risks related to Money Laundering and Financing of Terrorism,* 2017
2. Directive 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
3. FATF, *Best Practices Paper to Recommendation 2: Sharing among Domestic Competent Authorities Information related to the Financing of Proliferation*, 2012,
4. FATF, *Combating Proliferation Financing: A Status Report on Policy Development and Consultation*, 2010
5. FATF, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*, High level principles and procedures, 2007
6. FATF, *The FATF Recommendations, 2012*
7. International Federation of Accountants*, International Standards on Auditing*
8. OECD, *Bribery Awareness Handbook for Tax Examiners*, 2009
9. Paolo Mauro, *Why Worry About Corruption?,* 1997, IMF Economic Issues
10. United Nations Office of Drugs and Crime and IMF, *Model Legislation On Money Laundering and Financing of Terrorism*, 2005
11. United Nations Security Council Resolutions, *1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), and 1929 (2010)*

12. *Uniform Framework for Preventing and Combating Fraud and Corruption*, September 2006
13. World Bank, *Procurement Guidelines and the Guidelines for Selection and Employment of Consultants,* 2014