### TABLE OF CONTENTS

A. INTRODUCTION .................................................................................................................. 2

B. PREVENTION OF FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING ............................................................................................................. 3
   1. MANAGING THE RISKS .............................................................................................. 3
   2. IMPORTANCE OF ‘KNOW-YOUR-CUSTOMER’ STANDARDS ................................. 4
   3. ESSENTIAL ELEMENTS OF KYC STANDARDS ........................................................ 5
   4. THE ROLE OF AUDIT COMMITTEE, COMPLIANCE AND OPERATIONAL RISK MANAGEMENT OFFICE, INTERNAL AUDIT AND EXTERNAL AUDITORS ............ 7

C. IDENTIFYING FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING ....................................................................................................................... 8

D. FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING REPORTING & INVESTIGATION ..................................................................................... 9

E. ABOUT FRAUD AND CORRUPTION ............................................................................... 11
   1. WHAT IS FRAUD? ..................................................................................................... 11
   2. COMMON FRAUDS .................................................................................................. 12
   3. WHAT IS CORRUPTION? .......................................................................................... 13
   4. CAUSES OF CORRUPTION ....................................................................................... 14
   5. CORRUPT PRACTICES .............................................................................................. 14
   6. POLITICALLY EXPOSED PERSONS (PEPS) ............................................................ 15

F. ABOUT MONEY LAUNDERING ......................................................................................... 17
   1. WHAT IS MONEY LAUNDERING? ............................................................................... 17
   2. WHAT ARE THE TYPICAL CRIMINAL ACTIVITIES FROM WHICH PROCEEDS ARISE? .............................................................................................................................. 18
   3. HOW IS MONEY LAUNDERED? ................................................................................. 18

G. IMPACT OF FRAUD, CORRUPTION AND MONEY LAUNDERING ON ECONOMIC DEVELOPMENT .................................................................................................................. 20

H. ABOUT TERRORISM FINANCING ....................................................................................... 21
   1. WHAT IS TERRORISM FINANCING? ........................................................................... 21
   2. THE LINK BETWEEN MONEY LAUNDERING AND TERRORISM FINANCING ............ 22
   3. COMBATING FINANCING OF TERRORISM ............................................................... 22
A. INTRODUCTION

The fight against fraud, corruption, money laundering and terrorism financing\(^1\) ("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.

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:

i) has developed this Policy and associated procedures, and

ii) is committed to working and co-operating with other organizations to prevent organized 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 officials, staff, and counterparties -including its Directors, Alternate Directors, Temporary Alternate Directors, President, Vice Presidents, Secretary General, Officers, employees, consultants, contractors, counterparts 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 on 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.

\(^1\) For an elaboration on the concepts underlying these terms refer to chapters E, F and H, respectively, in this Policy.
B PREVENTION OF FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING

1. Managing the Risks

BSTDB 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 its governing bodies, President, Vice Presidents, Secretary General, Officers and employees, consultants and contractors can work and 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 programme rather than dealt with in isolation.

An effective FCMLTF prevention strategy and its implementation require the Bank’s Management (President/ Vice Presidents/ Secretary General) to:

- Identify the areas within the business most vulnerable to the risks of FCMLTF
- Enhance what processes are 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. A control system, which may have been effective on its introduction, may no longer fit readily with the latest organizational structure or meet the organization’s changing circumstances or needs.

The Bank’s Management (President/ Vice Presidents/ Secretary General) has 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 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 is employed, following the Bank’s relevant procedures. Additionally, a system of personnel management designed to deter staff from committing or tolerating FCMLTF should be in place.
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 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, especially 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 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 potential 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 programme. 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’ programmes, 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, etc.
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 organizes employee-training programs so that bank staff is 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. New staff 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 ongoing basis and to detect patterns of suspicious activity. Regular refresher training will be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within the Bank that promotes such understanding is the key to successful implementation.

3. Essential Elements of KYC Standards

a. KYC Procedures

KYC procedures will embrace routines for the proper management oversight, systems and controls (e.g. Customer Due Diligence -CDD-), segregation of duties, training and other related policies. The results of the CDD, including also an assessment of and expression of an opinion on the customers’ anti-fraud, corruption, money laundering, terrorism financing and integrity status, shall be reflected in the Bank’s operations approval documents. A CDD shall also be performed for any bank that is not listed and traded on a recognized stock exchange that is subject to disclosure requirements consistent with best international standards, before BSTDB 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\(^2\), KYC procedures will follow a risk-based approach enabling subjecting of customers to proportionate controls and oversight.

b. Customer and Beneficial Owner Identification, Verification and Record-Keeping

With regard to the Customer and Beneficial Owner Identification, Verification and Record-keeping Rules the Bank has adopted the related recommendations of the FATF, the measures which the FATF 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:

\(^2\) Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing, High level principles and procedures, June 2007
c. Documents Retention Period
All units should maintain, for at least seven years (Please refer to the Bank’s Rules and Procedures for the Management of Official Records and Archives), 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) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

Records on customer identification (e.g. documents referring to the legal status or the activity of our counterparts, banks or corporations), and business correspondence should be kept for at least seven years after the relationship is terminated.

d. New Technologies
Special attention should be paid to money laundering threats inherent in new or developing technologies that might favour anonymity, and measures should be taken, if needed, to prevent their use in money laundering schemes.

e. 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 BoD and any third party the which the Bank may decide to disseminate the information.

f. 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.

g. 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
h. Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the “correspondent bank”) to another bank (the “respondent bank”). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. The Bank shall gather sufficient information about a respondent bank to understand fully the nature of its business.

4. The role of Audit Committee, Compliance and Operational Risk Management Office, Internal Audit and External Auditors

Management has overall responsibility for ensuring the security and integrity of the assets of the Bank by putting in place appropriate controls and review procedures. For the effective countering of the threats of FCMLTF, all Management and staff have to take responsibility for their prevention and detection. The Bank’s Audit Committee, Compliance and Operational Risk Management Office (“CORMO”), Internal Audit Department, and its External Auditors will assist Management in preventing and detecting these threats within the framework of their responsibilities. CORMO has the responsibility to evaluate and ensure adherence to KYC policies and procedures. Internal Audit 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.

---

3 Basle Committee on Banking Supervision – Customer Due Diligence for Banks
4 Basle Committee on Banking Supervision – Customer Due Diligence for Banks
C. IDENTIFYING FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING

The Bank expects all its Directors, Alternate Directors, Temporary Alternate Directors, President, Vice Presidents, Secretary General, Officers, employees, consultants, contractors, counter-parts 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, 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.
D. FRAUD, CORRUPTION, MONEY LAUNDERING AND TERRORISM FINANCING REPORTING & INVESTIGATION

It is the responsibility of all staff 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, coercive, collusive or corrupt practices and of money laundering or terrorism financing may also be highlighted as a result of specific Management checks, by a third party, CORMO, or in the course of audit reviews by both internal and external audit.

If there is any uncertainty as to whether an action could constitute FCMLTF, CORMO should be contacted for guidance.

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 FCMLTF should be reported, if raised internally, or directed, if communicated to the Bank from external sources or through the Bank’s dedicated mechanism, to CORMO, which, in consultation with the General Counsel, will establish the course of action for each reported suspicion. If necessary, CORMO will establish, maintain and follow a FCMLTF Response Plan. The reported suspicion, however innocent, will be reviewed, analyzed and potentially investigated. If there is suspicion that a member of CORMO may be involved in FCMLTF the President and the Head of the Internal Audit Department should be informed instead.

Reporting persons or entities are encouraged to submit written allegations 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 FCMLTF.

Staff members, entities or individuals who come forward in good faith with reasonable suspicions or evidence of occurrences of illegal, unethical or questionable practices constituting internal or external fraud, internal or external corruption, money laundering or terrorism financing (whistleblowers) or cooperate or provide information during an ensuing review or investigation, shall be protected from unauthorized disclosure by the Bank of their involvement, unless such disclosure is required to proceed with an inquiry, or is necessary for proceedings under the Bank’s
Disciplinary Measures and Procedures or the Grievance Procedures. 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.

A staff member who acts maliciously, by disclosing information to CORMO that he 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, CORMO’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- to Board of Directors of the Bank, which in turn will decide about reporting it to the competent authorities. Every Member State will be requested to provide information about its local 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 terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to their competent authorities and notify the Bank accordingly.

Directors, Alternate Directors, Temporary Alternate Directors, President, Vice Presidents, Secretary General 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 CORMO, Internal Audit Department, the Bank’s President, B.o.D. or the competent authorities, comprising the authorities of the Bank’s Member States and international organizations such as INTERPOL.
E. ABOUT FRAUD AND CORRUPTION

1. What is fraud?

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 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 Financial Institutions Anti-Corruption Task Force and the World Bank:

- A fraudulent practice is any act 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.

- Obstructive Practice is i) 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 ii) acts intended to materially impede the exercise of the Bank’s investigation and audit rights.

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.

5 Uniform Framework for Preventing and Combating Fraud and Corruption, September 2006
6 Procurement Guidelines and the Guidelines for Selection and Employment of Consultants
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 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 complete outsourcing of key functions) in areas such as IT, accounting, contract tendering, and other professional services.

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.

**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.
b. Suppliers taking advantage of their customers (the latter being either BSTDB 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 taking back-handers 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 bypass 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.

3. What is corruption?

Corruption is a term associated with various illegal or immoral activities or behaviors. 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. 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. 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.

5. Corrupt Practices

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

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

i) 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.

---

7 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. Why Worry About Corruption?, Paolo Mauro, 1997, IMF.
8 Uniform Framework for Preventing and Combating Fraud and Corruption, September 2006
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 favors.

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.

ii) 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.
- 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 behavior.

iii) Organized fraud and 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.

6. Politically Exposed Persons (PEPs)

Business relationships with individuals 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 Senior Management or beneficial owners, 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 or other requests.

Any business relationship of the Bank involving interests of a PEP who otherwise has a direct relationship 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, senior management’s specific approval for establishing business relationships with such customers shall be obtained (at the appropriate committee level, be it Credit Committee, Management Committee or equivalent).
F. ABOUT MONEY LAUNDERING

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\(^9\), “Money laundering” includes the following:

- 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.

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.

2. **What are the typical criminal activities from which proceeds arise?**

- Drugs and psychotropic substances
- Terrorism
- Theft/Burglary/Robbery
- Kidnapping illegal restraint and hostage-taking
- Deception
- Corruption and bribery
- Fraud
- Participation in an organized criminal group and racketeering
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in stolen and other goods
- Counterfeiting and piracy of products
- Murder, grievous bodily injury
- Prostitution
- Forgery
- Blackmail
- Extortion
- Tax Evasion
- Evasion of Exchange Controls
- Smuggling
- Trafficking in human beings and migrant smuggling
- Illicit arms trafficking
- Counterfeiting currency
- Environmental crime
- Insider trading and market manipulation

3. **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.
G. IMPACT OF FRAUD, CORRUPTION AND MONEY LAUNDERING ON ECONOMIC DEVELOPMENT

Although historically some theorists have argued that corruption (and in some cases even fraud) was a natural stage of development or a means of transferring resources from wealthy individuals or entities to those of more modest means, it is widely accepted that both fraud and corruption hinder economic development, inter-alia, for the following reasons:

- 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
- they cause mistrust among communities hence hinder economic cooperation and development
- they increase the cost of the development process
- they diverge the allocation of scarce resources into unnecessary, uneconomic or illicit uses
- they create economic instability and divert foreign investments to more stable economies
- they lower asset life, as resources are directed away from maintenance toward new equipment and projects
- 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
- Corruption & fraud undermine laws, create disrespect for values and rules, and perceptions of unfairness- e.g. ‘he did it, why not me?’

In economic terminology, they increase transaction costs in an economy, increase real- and perceived- risks for undertaking economic activity and generate a ‘dead weight loss’ which increases inefficiency.

The activities of powerful criminal organizations can have serious social consequences. Laundered money provides drug traffickers, organized criminal groups, arms dealers and other criminals with the wherewithal for operating and developing their enterprises. 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.
H. ABOUT TERRORISM FINANCING

1. What is terrorism financing?

According to a widely accepted definition\(^{10}\) "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:

(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 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).

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 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.

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.

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 Money Laundering and Financing of Terrorism calls for the adoption of a consolidated strategy and approach. Several international, regional, and specialized bodies, among others the Financial Action Task Force on Money Laundering (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.