

## Anti-Fraud, Corruption and Money Laundering Policy

---

- A. INTRODUCTION
- B. ABOUT FRAUD AND CORRUPTION
  - 1. What is fraud?
  - 2. Common Frauds
  - 3. What is corruption?
  - 4. Causes of Corruption
  - 5. Corrupt Practices
- C. ABOUT MONEY LAUNDERING
  - 1. What is money laundering?
  - 2. What are the typical criminal activities from which proceeds arise?
  - 3. How is money laundered?
  - 4. How much “dirty” money needs to be laundered?
  - 5. Where does money laundering occur?
- D. IMPACT OF FRAUD, CORRUPTION AND MONEY LAUNDERING ON ECONOMIC DEVELOPMENT
- E. PREVENTION OF FRAUD, CORRUPTION AND MONEY LAUNDERING
  - 1. Managing the Risks
  - 2. Importance Of ‘Know-Your-Customer’ Standards
  - 3. Customer Identification And Record-Keeping
  - 4. The role of Audit Committee, Internal Audit and External Auditors
- F. IDENTIFYING FRAUD, CORRUPTION AND MONEY LAUNDERING
- G. FRAUD, CORRUPTION AND MONEY LAUNDERING REPORTING & INVESTIGATION

## **A. INTRODUCTION**

The fight against fraud, corruption and money laundering is central to the Bank's mission that is the promotion of regional development and co-operation.

In the spirit of the Agreement Establishing the Bank and according to its Financial Policies and international best practice, the Bank has the obligation to establish policies, procedures and systems of internal control to address the risks arising from fraud, corruption and money laundering.

The Bank is committed to ensuring that the risks of fraud, corruption and money-laundering are reduced to the lowest possible levels. Where there is the possibility of fraud, corruption or money-laundering, the Bank will deal with it in a decisive, timely and controlled manner.

Within this framework, the Bank:

- i) has developed these policies and associated procedures, and
- ii) is committed to working and co-operating with other organizations to prevent organized fraud, corruption and money-laundering. Wherever possible, the Bank will seek to co-operate and exchange information with the relevant competent authorities of its Member States, and with competent international organizations such as the Financial Action Task Force on Money Laundering of OECD<sup>1</sup>, the International Chamber of Commerce<sup>2</sup> and the Basel Committee of the Bank for International Settlements, in order to assist in combating fraud, corruption and money laundering, primarily within the region of its operations.

The Bank expects all its Directors, Alternate Directors, President, Vice Presidents, Secretary General, Officers, employees, consultants, contractors, counter-parts and customers to observe the highest standards of ethics and to provide the Bank with any help, information and support in combating fraud, corruption and money-laundering.

## **B. ABOUT FRAUD AND CORRUPTION**

### **1. What is fraud?**

There is no precise, universal, legal definition of fraud and no single criminal offence that can be called fraud<sup>3</sup>. It is usually taken to involve theft – the removal of cash and assets to which the fraudster is not entitled – or false accounting- falsification or alteration of accounting records or other documents.

---

<sup>1</sup> In response to mounting concern over money laundering, the Financial Action Task Force on money laundering (FATF) was established by the G-7 Summit in Paris in 1989 to develop a coordinated international response. FATF is a multi-disciplinary body -as is essential in dealing with money laundering- bringing together the policy-making power of legal, financial and law enforcement experts. Additionally, in 1997, the OECD approved and ratified a convention and full set of recommendations for criminalizing transnational bribery, enacting stricter accounting requirements and external and internal audit controls, tighter public procurement, and enhanced international controls.

<sup>2</sup> In 1998, the International Chamber of Commerce approved revised rules of conduct that prohibit bribes and recommended that its member associations around the globe, and their member corporations, adopt and apply these tighter rules.

<sup>3</sup> Section 2 of the Bank's Procurement Policies and Rules addresses fraud and corruption in the context of procurement using bank financing and defines these two terms consistent with harmonized documentation of the Multilateral Development Bank's.

A business or organization may be exposed to:

- external fraud, perpetrated by individuals outside the organization
- internal fraud, perpetrated by Management or employees
- collusion, between someone within the organization and an outsider.

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.

The threat of fraud has always existed, however, the opportunities for it may now be expanding:

- An increasingly educated workforce may be able to overcome a company's internal controls.
- Desk-top publishing means that 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.
- There may be a greater risk if a business is rapidly expanding.
- Organizations may be more prone to cost-cutting than in the past, but is the cost/benefit always analyzed? This may result in fewer people in Management with fewer controls.

## 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 danger from fraud may come from four broad categories:

#### a. Employees abusing their position:

- The misappropriation of assets (such as cash, stock, reimbursement of expenses, payroll, stationery, etc.)
- 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.
- Employees taking unwarranted sick leave could be classified as fraud. However, this sort of behavior would not be reported to outside authorities. The onus would be on Management to monitor and deal with the situation.

b. Suppliers may take advantage of their 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 by-pass due diligence controls in order to obtain credit that will not be repaid.
- More significant frauds may occur if employees collude with either suppliers or customers.

d. Computer 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.
- New technological developments may present a whole new range of threats.

### 3. What is corruption?

Corruption is a term associated with various illegal, illicit or immoral activities or behaviors. In the context of banking and International Financial Institutions, corruption could be defined as the abuse of official 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 (see also footnote 3, p.3).

### 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
- Lack of transparency and inadequate communication channels
- Low wages of staff, limited job satisfaction or an unfair remuneration/ benefits system

Public corruption can be mainly traced to government intervention in the economy. Hence policies aimed at liberalization, stabilization, deregulation, and privatization can sharply reduce the opportunities for corrupt behavior. Where government regulations are pervasive, however, and government officials have discretion in applying them, individuals are often willing to offer bribes to officials to circumvent the rules. Identifying such policy-related sources of corruption is

obviously helpful in bringing it under control. The following sources of corrupt practices have for some time been well known:

- Trade restrictions are the prime example of a government-induced source of corrupt practices
- Government subsidies
- Price controls, whose purpose is to lower the price of some good below its market value (usually for social or political reasons)
- Multiple exchange rate practices and foreign exchange allocation schemes lead to corrupt practices
- Low wages in the civil service relative to wages in the private sector
- Natural resource endowments (oil, gold, exotic lumber) - since they can typically be sold at a price that far exceeds their cost of extraction and their sale is usually subject to stringent government regulation, to which corrupt officials can turn a blind eye.

## 5. Corrupt Practices

Corrupt practices and consequently the efforts to combat corruption may broadly rest upon the following three pillars (with illustrative examples 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.
- 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.

**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.

## **C. 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.

These criminal acts can generate huge sums. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits 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 the European Commission's Directive<sup>4</sup>, "Money laundering" means 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 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 abovementioned activities may be inferred from objective factual circumstances.

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

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

Drugs	Prostitution
Terrorism	Forgery
Theft/Burglary	Blackmail
Kidnapping	Extortion

---

<sup>4</sup> Directive 2001/97/EC of the European Parliament and of the Council – 4 December 2001

Deception  
Corruption  
Fraud

Tax Evasion  
Evasion of Exchange Controls

### **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. Establishing and maintaining the Bank's good reputation is of paramount importance.

### **4. How much "dirty" money needs to be laundered?**

There are no accurate statistics for the amount of criminal money needing to be laundered. However a former Managing Director of the IMF estimated the figure to be two to five percent of the world's gross domestic product. This would be around one Trillion \$ annually.

### **5. Where does money laundering occur?**

As money laundering is a necessary consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out areas in which there is a low risk of detection due to weak or ineffective anti-money laundering programmes. Because the objective of money laundering is to get the illegal funds back to the individual who generated them, launderers usually prefer to move funds through areas with stable financial systems.

Money laundering activity may also be concentrated geographically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the underlying activity; often, but not in every case, in the country where the funds originate.

With the layering phase, the launderer might choose an offshore financial centre, a large regional business centre, or a world banking centre –any location that provides an adequate financial or business infrastructure. At this stage, the laundered funds may also only transit bank accounts at

various locations where this can be done without leaving traces of their source or ultimate destination.

Finally, at the integration phase, launderers might choose to invest laundered funds in other locations if they were generated in unstable economies or locations offering limited investment opportunities.

#### **D. 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

Regarding money laundering, 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.

Differences between national anti-money laundering systems will be exploited by launderers, who tend to move their networks to countries and financial systems with weak or ineffective countermeasures.

#### **E. PREVENTION OF FRAUD, CORRUPTION AND MONEY LAUNDERING**

##### **1. Managing the Risks**

In order to defeat fraud, corruption and money laundering, we must 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 that its President, Vice Presidents, Secretary General, Officers and employees, consultants and contractors can work and its project and trade financing and other activities will be conducted.

The management of fraud, corruption and money laundering 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 fraud, corruption and money laundering 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 fraud, corruption and money laundering

- Establish what processes are already in place
- Identify extra or alternative controls needed to reduce these risks
- Introduce the extra or alternative controls to prevent fraud, corruption and money laundering 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 President/ Secretary General) are responsible for the proper implementation of this policy in their respective Divisions. They must ensure through regular control and risk self-assessments that suitable controls to prevent fraud, corruption and money laundering 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 fraud, corruption and money laundering.

As most fraud, corruption and money laundering experienced by an organisation is committed or tolerated by its own staff, hence when new staff is employed, following the Bank's relevant procedures, a check of references and previous employment records must be made. Additionally, a system of personnel management designed to deter staff from committing or tolerating fraud, corruption and money laundering 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 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 (e.g. the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, 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 so easily become a vehicle for or a victim of illegal activities perpetrated by

their customers. They need to protect themselves by means of continuous vigilance through an effective KYC programme. Assets held on a fiduciary basis, such as Special 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 lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the Bank. Banks may become subject to lawsuits resulting from the failure to practise due diligence. Consequently, the Bank can, for example, suffer fines, criminal liabilities and special penalties. Indeed, a court case involving the Bank may have far greater cost implications for its business than just the legal costs. The Bank will be unable to protect itself effectively from such legal risks if it does not engage in due diligence in identifying its customers and understanding their business.

Supervisory concern about *concentration risk* mostly applies on the assets side of the balance sheet. 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 a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

KYC procedures will embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies.

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

The Bank will establish an ongoing employee-training program 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. Customer Identification And Record-Keeping**

With regard to the Customer Identification and Record-keeping Rules the Bank has adopted the related recommendations of the FATF, the measures which the Task Force have agreed to implement and which all countries are encouraged to adopt.

These Recommendations set out the basic framework for anti-money laundering efforts and they are designed to be of universal application:

#### **a. Verification of Legal Existence and Structure**

In order to fulfil identification requirements concerning legal entities, the Bank should take measures:

- to verify the legal existence and structure of the customer by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity.
- to verify that any person purporting to act on behalf of the customer is so authorised and identify that person.

**b. *True Identity of Customers***

The Bank should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction conducted if there are any doubts as to whether these clients or customers are acting on their own behalf, for example, in the case of domiciliary companies (i.e. institutions, corporations, foundations, trusts, etc. that do not conduct any commercial or manufacturing business or any other form of commercial operation in the country where their registered office is located).

**c. *Documents Retention Period***

All units should maintain, for at least seven years (retention period will be dealt with in more detail in a Documents Retention Policy to-be-issued), all necessary records on transactions, *both domestic or international*, 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), credit files 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 Bank will decide to disseminate the information.

If suspicion will arise that funds stem from a criminal activity, it should be promptly reported to Internal Audit.

**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.

#### **4. The role of Audit Committee, 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.

The Bank's Audit Committee, Internal Audit Department and its External Auditors will assist Management in preventing and detecting fraud, corruption and money laundering within the framework of their responsibilities, however, for the organization to be effective in countering the threats of fraud, corruption and money laundering, all Management and staff have to take responsibility for their prevention and detection.

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.

#### **F. IDENTIFYING FRAUD, CORRUPTION AND MONEY LAUNDERING**

The Bank expects all its Directors, Alternate Directors, President, Vice Presidents Secretary General, Officers, employees, consultants, contractors, counter-parts and customers to observe the highest standards of ethics and to have a responsibility for fraud and corruption prevention 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 and detecting fraud, corruption and money laundering. Fraud, corruption and money laundering prevention and detection matters shall be included in the Bank's induction programs and continuous career training.

#### **G. FRAUD, CORRUPTION AND MONEY LAUNDERING REPORTING & INVESTIGATION**

It is the responsibility of all staff to stay alert for occurrences of fraud, corruption or money laundering and to be aware that unusual events, transactions or behaviors could be indications of actual or attempted fraud, corruption or money laundering.

Fraudulent or corrupt practices may be highlighted as a result of specific Management checks, by a third party, 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 fraud, corruption or money laundering, the Internal Audit Department should be contacted for guidance.

The Internal Audit Department will establish, maintain and follow a Fraud, Corruption and Money Laundering Response Plan in co-operation with the Office of the General Counsel. Any suspicions of fraud, corruption or money laundering should be reported to the Internal Audit Department, and however innocent, will be reviewed, analyzed and potentially investigated. If there is suspicion that a member of the Internal Audit Department may be involved in fraud, corruption or money laundering the Office of the President should be informed instead.

If it will be deemed that there is serious evidence of fraud, corruption or money laundering, then the issue will be reported -through the Bank's Management- to B.o.D., 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.

Directors, Alternate Directors, President, Vice Presidents, Secretary General, Officers and employees will be protected by specific provisions from liability for breach of any restriction on

disclosure of information imposed by contract or by any internal regulation, if they report their suspicions in good faith to the competent authorities. In case provisions of this policy contradict the provisions of any other regulation (including but not limited to the Policy on Disclosure of Information and Confidentiality), the provisions of this policy will prevail.

Directors, Alternate Directors, President, Vice Presidents, Secretary General, Officers and employees, are not allowed to warn any of the suspected parties or anyone else associated with them when information relating to them is being reported to Internal Audit, B.o.D. or the competent authorities, comprising the authorities of our Member States and international organizations such as INTERPOL.