















Prevention of money laundering and terrorist financing system self-assessment form

In accordance with the guide on recommendations on internal control of PML/TF issued by SEPBLAC and published on its website, we have prepared this **self-assessment form for the PML/TF system**. As with the internal control recommendations document, the subject parties must adapt this form to the realities of their business and the PML/TF risks faced.




All assessments should be made with regard to a specific standard, represented by current regulations at the time and the internal control measures they set out. In this case, the recommendations guide, which has been designed to facilitate compliance with these measures, establishes a reference standard to self-assess the effectiveness of the money laundering prevention system for each subject party.

The self-assessment form is divided into four main sections: governance; due diligence; detection, analysis and communication; and system review (internal audit and external experts). These four sections are in turn broken down into a number of subsections. Assessments of these is colour coded (green: satisfactory compliance; amber: substantial progress on measures taken; red: need to implement appropriate measures). To make it easier to complete the self-assessment form, the accompanying appendix sets out a number of points to develop each of these subsections.

Prevention of money laundering and terrorist financing self assessment form

		Assessments *
		2012
Governance	Involvement of senior management: information provided and frequency	
	Composition of the OCI (Internal Control Body): representation and functionality	
	Prevention unit: Structure and functions	
Due diligence	Customer acceptance policy	
	Customer segmentation and additional measures	
	Identification: real beneficiary	
	Knowledge: activity, source of funds	
	Document archiving: digitalisation	
Detection, Analysis and Communication	Functionality of the detection tool	
	Alert management	
	Internal employee communication	
	Special analysis process	
Reviews	Internal audit	
	External expert	

Assessments:

Satisfactory compliance: no need for significant additional measures

Substantial progress in implementing measures taken

Need to implement appropriate improvements

* Note: the assessments shown in the form are for illustration purposes only

Issues to consider when filling in the PML/TF prevention system
self-assessment form

1. GOVERNANCE

a. Involvement of senior management (Board or Board Committees): information provided and frequency.

- Information and/or documentation for the entity's senior management on PML/TF issues. The frequency with which senior management is informed of such issues
- Senior management attendance at PML/TF training courses. Decisions taken by senior management

b. Composition of the OCI (Internal Control Body): representation and functionality.

- Areas represented in the OCI
- Frequency of meetings
- Meeting dynamics, attendance of technical staff, information addressed, agility in decision making
- Delegation of functions to the unit or other subcommittee

c. Prevention unit: structure and functions

- Assessment of the adequacy of the Prevention Unit's human resources in the context of the functions assigned to it, and those delegated by the OCI if any
- The degree of autonomy for performing its functions with agility

2. DUE DILIGENCE

a. Customer acceptance policy

- Adequate controls for detecting persons or entities whose approval is not permitted; process for consulting internal and international lists

b. Customer segmentation and additional measures

- Definition and application of customer segmentation based on risk and characteristics
- Performance of the IT tool assigning risk levels to the customer based on the data obtained when establishing the business relationship. Back-feeding customer transactions into the system
- Progressive additional measures (authorisations, additional documentation required, etc.) based on risk level assigned to the customer

c. Identification

- General automatic identification controls
- Procedures to ensure that the real beneficiaries are correctly identified in all transactions

d. Knowledge: source of funds

- Content of KYC files
- Procedures for verifying sources of funds
- Automatic documentation controls on activity based on risk levels
- Effectiveness of abstention from execution

e. Document archiving: digitalisation

- Document digitalisation system

3. DETECTION, ANALYSIS AND COMMUNICATION

a. Functionality of the detection tool

- Risk transactions defined in the tool. Inclusion of all the entity's business areas
- Consideration of risk profile assigned to the customer for purposes of checking fit with customer transactions
- Changes to customer's usual behaviour

b. Tool alert management

- Generation of alerts: frequency and response periods
- Performance of the alert management process: participation of prevention unit, branches and other departments. Checks required
- Exceptions for recurrent transactions. Authorisations required, duration

c. Internal employee communications

- Performance of internal communication system for suspicious transactions
- Relevance of communications by employees. Percentage of transactions finally reported to the Executive Service
- Assessment of the weight of employee communications compared to all of the entity's communications to the Executive Service
- Inclusion of case studies in prevention training

d. Special analysis process.

- Definition of transactions subject to special analysis. Statistics
- Performance of decision-making process for special analysis of transactions. Period
- Special operations database: periodic reports
- Definition and percentage of transactions in ongoing monitoring
- Documentation of special analysis process. Reasons for decision not to communicate transactions

4. REVIEWS

a. Internal audit.

- Internal audit plan. Scope of PML/TF audits: business lines, processes, tools, etc. Frequency of reviews
- Communication of audit results to competent bodies. Weakness correction control
- Improvements to PML/TF system as a result of audit reports

b. External expert.

- Assessment of the external expert's report. Weaknesses highlighted
- Communication of results to competent bodies. Weakness correction control
- Improvements to the PML/TF system as a result of the report