Recommendations on internal control measures for prevention of money laundering and terrorist financing.

In line with international standards, Spanish regulations on the prevention of money laundering and terrorist financing (PML/TF) establish a requirement for subject parties to have in place adequate prevention procedures and bodies.

Article 26 of Act 10/2010 on prevention of money laundering and terrorist financing sets out a series of internal control obligations, subject to certain exceptions. These obligations include approving and applying prevention policies and procedures; setting up adequate internal control bodies responsible for applying these policies; and approving a prevention manual.

In order to help subject parties comply with article 26 obligations, and the framework set out in article 45.4.g) of Act 10/2010, SEPBLAC has prepared this document of recommendations on internal control measures for PML/TF. This is not a regulation in the strict sense, but rather a guide that must be adapted to the reality of each subject party.

This document briefly summarises the regulatory framework, sets out some general principles and then provides a more detailed section of specific internal control recommendations. This document is largely based on accumulated experience in the supervision of reporting of suspicious transactions by subject parties, the supervisory actions carried out and assessment of prevention procedures in the context of administrative authorisations, in which SEPBLAC has a mandatory role in pronouncing on the adequacy of internal control measures related to prevention.

Article 2 of Act
10/2010 covers a wide range of very varied subject parties. These all have very different degrees of exposure to money laundering and terrorist financing risks, as they operate in different sectors and these offer different routes for introducing funds into the legal system. The greater the risk, the more sensitive subject parties must be, and the more robust their control and prevention mechanisms must be.

Effectiveness in the context of PML/TF means society -in our case, Spain- having solid, comprehensive barriers to introducing the proceeds of crime into the legal economy: these barriers need to be more than just a formality. Economic crimes -aiming to profit from illegal activities- are inherent to society, and many measures of various natures have been established to combat them (legislative, administrative, police, legal, criminal, prisons, etc.). We have to do everything in our power to stop the enjoyment of illicit gains.

SEPBLAC aims to contribute to this objective through the recommendations in this document, which sets out principles that are easy to describe but difficult to implement and put into practice effectively. There can be no doubt that this is an ambitious objective. And it is something that everyone must be committed to, as those seeking to launder illicit funds can easily identify the weakest links in the chain of a country's prevention system.

The first requirement for subject parties to be able to carry out effective prevention is for them to be aware of their own risks. Therefore, the first principle set out in the section on general principles is focusing on risk, referring to the need for all subject parties to complete a "risk self-assessment form". This is set out in more detail in section 3.1 of the recommendations document. This is not a technical prevention report. Rather, it is a practical report that adapts to the reality of the activity of each subject party, providing a health check for the business from the perspective of money laundering. Using this approach helps to identify the risks of someone exploiting the activity of the subject party to introduce, move or hide funds from suspicious sources. Nobody understands the risks of a business better than the people who run it. We start from the basis that those who are professionally involved in an activity are best placed to distinguish the normal from the unusual.

It is possible that some, or indeed many, of the recommendations herein may not apply to some subject parties: this is precisely because of the diversity of subject parties and the different levels of risk they face. Every subject party must adapt these recommendations to their own specific case.

Establishing prevention and control measures for a country is costly and complex: that is why we must focus on the effectiveness of the controls. We will not have achieved anything if we implement formal procedures but they are not effective.

SEPBLAC

The **Executive Service** of the Commission
for the Prevention of Money Laundering and
Monetary Offences

4.04.2013

Recommendations on internal control measures for the prevention of money laundering and terrorist financing

TABLE OF CONTENTS

Introduction

Article 2 of Act 10/2010, of 28 April, on the prevention of money laundering and terrorist financing (hereinafter, PML/TF) lists a wide range of subject parties, both in terms of their number and their type of activity.

These subject parties face very different risks and degrees of exposure to money laundering and terrorist financing. This risk is subject to both quantitative and qualitative factors linked to the activity of the subject party. It is obvious that the risks faced by a large bank with thousands of branches in varied locations and involved in a wide range of activities (retail, corporate, private, business banking, etc.) are very different those of a family jewellery business in a small town.

Therefore, the internal control structures, procedures, tools and resources to be applied by the different subject parties must be adapted to their differing risks.

The pillars of ML/TF prevention contained in the due diligence measures set out in articles 3 to 7 of the Act (identification of the formal and real beneficiary, understanding their activity and the source of the funds that the customer seeks to channel through the subject party) are based on this risk approach.

Likewise, the internal control measures set out in article 26 of the Act, which the subject parties must establish and apply, must be consistent with the degree of risk they face. Therefore, article 26 allows for certain exceptions to the generic obligation to approve and apply prevention policies and procedures, specifically with regard to having an express client acceptance policy, communication to the Executive Service of proposed appointments of representatives to communicate with the Service, approval of a manual and the formation of a technical prevention unit.

These recommendations must be considered in the context of this risk-based approach, in particular, the preparation of an ML/TF risk self-assessment report (sections 2.1 of the general principles and 3.1.a) of the recommendations). This self-assessment report is not a technical money laundering prevention report; rather, it must be adapted to the business. However, it must be prepared from an ML/TF perspective. The conclusion of this report will be the degree of risk to which the subject party is exposed, and the appropriate resulting measures to take.

For the purposes of preparing this report, the risk assessment should be based on the objective elements set out in point 3.1.a) of the recommendations, such as the sector of activity, the size of the business, the number of employees, the areas in which it works, the average number of employees and where they come from, nationalities and countries involved in the transactions, the use of agents in transactions, etc.

The other measures included in the recommendations document should be adapted by the subject party based on the ML/TF risk of their business.

The purpose of these recommendations is to help subject parties to comply with the obligation to have in place policies, procedures and an adequate manual on prevention of money laundering and terrorist financing.

1. Regulatory framework

Article 26, section 1 of Act 10/2010 establishes, that the *institutions and persons covered by [the] Act,* ***with the exceptions determined in the regulations****[1], shall adopt in writing and implement adequate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing*.

Section 3 of this article further establishes that *institutions and persons covered by [the] Act,* ***with the exceptions determined in the regulations****, shall adopt an appropriate manual for the prevention of money laundering and terrorist financing, which shall be kept up to date with complete information on the internal controls referred to in the article*.

Likewise, article 45.4.i) of Act 10/2010 empowers the Executive Service of the Commission to *Report, with the exceptions determined in the regulations, on the procedures for the creation of financial institutions and on the adequacy of internal controls under the schedule of activities*.

Meanwhile, Act 5/2009, of 29 June, on the reform of the system for qualifying holdings in credit institution, investment firms, and insurance companies, establishes that sector supervisors (the Banco de España, the National Securities Market Commission (CNMV) and the Directorate General of Insurance and Pension Funds) must, in procedures relating to the acquisition of qualifying holdings, request a report from the Commission's Executive Service assessing the existence of indicators that the proposed acquisition is, has been, or is intended to be for the purposes of laundering money or financing terrorism, or that it could increase such risks.

Therefore, these recommendations on internal control measures for the prevention of money laundering and terrorist financing have been prepared to meet this need and to exercise the competence attributed to the Commission's Executive Service under article 45.4.g) of Act 10/2010, to *make recommendations to institutions and persons covered by this Act in order to improve internal controls*.

The PML/TF policies, procedures and manuals established by the subject parties shall likewise be subject to effective implementation and adaptation to the actual activities of the subject party, and to subsequent assessment by the Commission's Executive Service in exercise of its supervision functions.

1 These recommendations have been prepared in accordance with the provisions of Act 10/2010 but prior to its implementing regulations; therefore, once these have been approved, the exceptions and other aspects set out therein must be taken into account.

2. General principles

2.1 Risk-based approach
Subject parties shall develop their prevention procedures based on the ML/TF risks inherent to their activity and how they operate

When preparing, developing and applying their prevention policies, procedures and manuals, subject parties must take into account and adapt the measures set out in section 3 **based on the ML/TF risks** inherent to the nature of their activity, the sector in which they operate, their relative size, business practices, their customer base, cash handling, the geographic area in which the operate, etc.

In this regard, Act 10/2010 amended Spanish regulations on prevention, introducing a risk-based approach. This aimed to ensure that this approach is correctly applied by all subject parties, so as to improve the efficiency of available resources, decreasing the load on all subject parties involved in the national prevention system.

Subject parties must prepare a document or report describing and assessing their exposure to ML/TF risks

In order to achieve an appropriate appreciation and understanding of ML/TF risks, **subject parties must prepare a highly practical document or report adapted to their business**, **describing and assessing their exposure to ML/TF risks** in their activities. This report, which provides a health check of the business from a PML/TF perspective, will identify the ML/TF risks that might affect the subject party's business. The length and depth of the document or report will depend on the level of risk in the subject party's activity. The minimum content for this document is set out in section 3.1.a) of this document. This assessment report on money laundering and terrorist financing risk shall be available to the Commission's Executive Service.

2.2 Raising awareness
Senior management must understand the ML/TF risks to which they are exposed and ensure that appropriate measures are taken to offset these

The subject party's senior management is responsible for PML/TF risk-management policies and procedures. This means that it **must understand the ML/TF risks** to which it is exposed, **ensuring that all necessary measures are taken to effectively offset such risks**. Therefore, the subject party's senior management must take an active role in the prevention system implemented.

The subject party's prevention procedures must be approved by a senior management body or manager

The subject parties' senior management must be involved in all PML/TF work. Therefore, the policies, procedures and manuals prepared, developed and implemented in this area must be approved by a member of senior management or a senior management body, irrespective of the size or turnover of the subject party.

2.3 Prevention focus
The prevention function is not the exclusive responsibility of technical prevention units, as these represent only the subject party's first filter

It must be understood that prevention, as with all obligations relating to customers, is not exclusively a task for technical prevention units, but is a function of all commercial units, the business network (retail, corporate, private, business banking, etc.) and all the various lines of activity, as it is the business areas that work with the customers, and which apply

the due diligence measures; therefore, they must take an active role in prevention work. **The first filter in the subject party's prevention system is establishing a relationship with customers.** This relationship is the responsibility of business units, who are the first line of defence against ML/TF.

Prevention procedures must not focus exclusively on the capacity to detect, analyse and communicate transactions with suspicious signs, but also on early detection of possible customers or operations that pose a risk

Subject parties must remember that the best form of defence against ML/TF is to prevent transactions related to these activities taking place in the first place, by implementing procedures for adequate prevention and enabling them to be anticipated. Therefore, the development and application of prevention procedures **should not focus exclusively on the capacity to detect, analyse and report suspicious transactions** once they have passed through the first filter; **it must also aim to detect those customers and transactions that pose a risk in advance** (e.g. through due diligence, internal organisation and control, training, etc.) so as to stop such transactions being carried out.

Technical prevention units are the front line in the prevention system, and senior management must therefore ensure that they have the resources they require

Technical prevention units have a key role in prevention, **being at the sharp end of the system** and fully dedicated to such tasks, and given the exacting qualification levels required for their roles. Technical prevention units must play a key role in maintaining a high level of awareness of prevention throughout the subject party. To this end, senior management must ensure that these units **have the technical and human resources they require** to carry out their prevention work. This should not be limited exclusively to detection, analysis and the reporting of transactions; these units must **take an active role in developing the prevention system,** including continuous assessment of the functioning of the prevention system and its effectiveness.

2.4 Feedback

A communication channel must be established between prevention bodies and business units for risks to which a subject party might be exposed, establishing the measures required to offset these

Subject parties must establish a responsive **feedback procedure between its prevention bodies and business units** for the risks they might be exposed to in their activities, putting in place the measures required to offset these. In particular, the prevention bodies must notify business units of the types of transactions that should not be accepted or implemented as they present **patterns or elements of risks common** to other transactions previously classified as being related to ML/TF or suspicious.

The procedure for disseminating such types of risk transactions to business units must ensure they are capable of detecting and stopping the execution of transactions displaying these risk patterns or elements. The purpose of the prevention function is fulfilled when a suspicious transaction does not occur, not just through detection, analysis and reporting of suspicious transactions.

2.5 Universality
The prevention protocols must be applied to all the subject party's customers, transactions and business areas, without exception

Subject parties should also be reminded of the **need to apply prevention protocols universally;** in other words, every customer with whom a business relationship is established, and all transactions and business areas in which they operate, whether regularly or on an occasional basis, must be subject to the prevention protocols in advance, based on analysis of the prevention risks involved in each. No customer, transaction or business area may be excluded from prevention policies, including, in particular, any transactions not originating from, or executed through, the usual business channels (e.g. corporate or occasional transactions related to special private banking customers, real estate sales, sales of loan portfolios, etc.).

2.6 Adaptation to the business
The procedures implemented must be fully adapted to the business and activities of the subject party

The wide diversity of parties subject to compliance with PML/TF regulations, and their differing characteristics, sectors, size, etc. mean that the **procedures, manuals and IT applications used must be fully adapted to the specific business areas in which they are involved** and the activities they perform, together with the products and services they offer or sell, the markets in which they operate, and the customers, suppliers, intermediaries, investors and agents with which they work.

2.7 The cornerstones of prevention
The prevention procedures must be based on determining the actual beneficiary, the source of the funds and the consistency of the transaction carried out

Based on the risk-based approach set out above, the **cornerstones** on which subject parties should base their PML/TF procedures are those that enable them to **determine the actual beneficiary of the transaction**, and to **understand the source of the funds used** by customers and the **consistency of the transactions carried out by the customer with the understanding that the subject party has of its activities, business profile and risk**. Therefore, prior to establishing any business relationship, subject parties should request and obtain all the information and documentation they need for the risk presented.

2.8 Enhanced monitoring of new customers, products and services
Subject parties must undertake enhanced monitoring of transactions with new customers, and when new products and services are involved

Based on the risk, subject parties must likewise enhance and apply additional prevention measures for **transactions with new customers, agents, correspondents, and so on,**and for **transactions involving new products and services** that they have not previously offered. These measures involve maintaining **special monitoring** from the time that a new business relationship is forged, or from the start of offering new products and services and for the period considered reasonable by the subject party, in order to verify their consistency with the activity performed and their understanding of the customer, agent, correspondent, etc.

Likewise, subject parties must, prior to offering new products or services, or entering new markets or establishing new business lines, **undertake**

analysis in advance of the ML/TF risk and impact of new products, services, markets and business.

2.9 Practical and responsive document

The prevention measures should not just be a transcription of current regulations. They must describe the procedures effectively implemented in practice

Likewise, the **prevention measures** prepared, developed and implemented by subject parties must be tailored to their operating reality at all times, and **not just be a mere transcription or copy of the generic obligations set out in current regulations.** Policies, procedures and manuals that do not relate to the operating reality of the subject can not be considered adequate; this is also true of policies, procedures and manuals that simply list prevention obligations, without specifying how these should be effectively applied in practice.

The prevention manual must adapt responsively to changes in the business and procedures

The **PML/TF manual** must be a **practical and responsive document**, not just a response to a formal requirement. It must enable effective implementation and must **adapt easily to the business** of the entity **and to changes in its procedures and its business**.

2.10 External review of the system

External prevention system reviewers should provide a reasoned opinion on the effectiveness of the system in general, and on all improvements and modifications required

External reviewers (such as the external expert and internal auditors) have an important role to play in assessing the subject party's prevention system. Their reports should not be limited to describing the functioning of the system, or individually assessing existing procedures. They should **provide a reasoned opinion on the effectiveness of the system in general, and on all improvements and modifications required**. To this end, they should collect the samples established in Order EHA 2444/2007, of 31 July, and such additional samples as they consider necessary for supporting their opinion. This will include an assessment of the due diligence measures established, handling of prevention alerts, the special analysis process and the reasons for decisions taken.

2.11 Updating and reviewing the procedures

Subject parties must keep a record of all updates to their procedures

To facilitate monitoring of changes to the prevention manual, **subject parties must keep a register of all changes** detailing changes made, the reasons for these and their dates.

The Executive Service may, when it considers necessary, review the adequacy of the procedures established by the subject parties and their implementation in practice

In performance of its supervision and assessment function for the internal control measures established or proposed, the **Commission's Executive Service may** at any time **review the adequacy of the subject party's procedures, internal control bodies and reporting**, further **assessing** in its inspection **their implementation in practice and their adequacy for the activity of the subject party**.

3. Recommendations on internal control measures for prevention of money laundering and terrorist financing

Section 2 sets out the recommendations that subject parties **should take into consideration when preparing their prevention manuals and procedures**. All of these control measures must be set out in as much detail as possible, including all the information needed to understand in depth their characteristics, functioning and application.

There is no requirement for the structure of prevention manuals to specifically follow the numbering and naming conventions in this section. The risk level is determined by the risk self-assessment form discussed in the following section. Nevertheless, in its supervision and assessment of the adequacy of the internal control measures established or proposed, SEPBLAC might consider the control procedures established inadequate, taking account of the characteristics and type of the business in which the subject party is involved, .

The purpose of this list is to provide guidance to subject parties on preparing and implementing their measures and manuals. It should not be considered exhaustive, as other aspects of PML/TF may also be relevant to the specific nature of the entity's activity.

3.1. The money laundering and terrorist financing risk self-assessment form

a) All subject parties, without exception, must prepare a practical document or report (the **ML/TF risk self-assessment form**) tailored to the needs of its business, identifying and assessing its exposure to ML/TF risks. This document or report shall serve as a health check of the business in terms of PML/TF, describing and analysing the risks that might affect the activities of the subject party, **expressly mentioning, at least**:

- Basic details of the subject party: identifying details; a general description of the activity and characteristics of the subject party from a PML/TF perspective; a description of any group to which it belongs, where appropriate; relationships to any branches or subsidiaries; any activities through agents or other intermediaries who market the subject party's products or through which it operates.

- The activities, products and services offered by the subject party, specifying those presenting the greatest ML/TF risk (e.g. international deposits or movement of assets and funds, products offering anonymity and use by third parties, private and counterpart banking services, products susceptible to subsequent resale, etc.).

- Systems and channels used to deposit, move and transfer funds, referring to the risk they pose (e.g. cash, credit and prepay cards, bearer cheques and cheques payable to order, domestic and international transfers, the possibility of remote transactions not requiring presence in person, etc.).

2 Throughout this section, any reference to *customers* should be understood in the widest sense to include all persons with whom the subject party has any business relationship, including clients, suppliers, agents, intermediaries, correspondents, etc.

- The type of customers, specifying those that might present the greatest prevention risk (e.g. new customers, non-resident customers, customers involved in businesses handling large volumes of cash, customers with complex ownership or control structures, customers involved in certain specific risk activities, etc.).

- The actions of customers that might present the greatest ML/TF risks (e.g. difficulties in application of due diligence measures, transactions with no obvious or business logic, transactions where it is difficult to determine the source of the funds, etc.).

- The geographic area of activity of the subject party, specifying those where the subject party is based or operates that pose the greatest risk (e.g. tax havens, countries subject to international financial sanctions, countries with high levels of corruption, countries with weak PML/TF regulations, etc.).

- Any other factors considered to be risks for prevention.

- The procedure in place to ensure that the risk assessment document or report is regularly reviewed and updated. These reviews and updates must take account of the development of the business and the activities of the subject party, together with external factors that might influence the risk assessment (e.g. new ML/TF methods, trends and products, changes to the list of countries considered to pose risks, etc.).

The **ML/TF risk self-assessment form** should form the foundation of the PML/TF system. The risks set out in the document should be the basis for designing appropriate measures and procedures to offset these effectively.

3.2. Internal regulations

a) A list of all current internal regulations, instructions, provisions and general documents issued by the entity relating to PML/TF.

b) The scope of the PML/TF manual: including a list of any group entities to which it applies. The body that approves the manual. The system for distributing the manual to employees, managers and employees of subsidiaries. **A register** of updates to the procedures manual, expressly setting out any changes made, the causes for these and their dates.

3.3. Internal organisation

a) The management bodies of the subject party, setting out their functions, powers and competencies in relation to PML/TF. The need to keep a **register** of documentation and reports submitted to such bodies and the decisions taken in relation to this issue.

b) The internal control body (OCI for the Spanish acronym) responsible for applying PML/TF policies and procedures, explicitly setting out, at least:

   - The composition and positions of the members in the subject party.

   - The hierarchical position of this body in the subject party's organisation chart and to whom it reports.

   - The frequency of meetings.

- The prevention functions allocated to it.

- The preparation and archiving of minutes of its meetings, which must contain full and sufficient information on all the issues dealt with and the resolutions adopted.

- A list of documents, reports, presentations, etc. relating to prevention sent to the governance bodies and senior management of the subject party.

- Regular issuance of a **report or explanatory note**, at least annually, setting out the most relevant statistical information on prevention and the actions implemented during the period (e.g. significant changes to procedures; implementation of new IT applications; statistical information on the number of alerts, transactions subject to special analysis, reports submitted to SEPBLAC, information requests or instructions received; the process for implementing improvements to the prevention system indicated by the external reviewer; etc.).

c) A description of the internal organisation of the group, and its existing bodies and reporting procedures with the bodies of subsidiaries, including those abroad, or between group companies.

d) The representative to SEPBLAC, explicitly stating their **management or administrative position** in the subject party, and the role they perform, indicating which of these have been delegated by the OCI. The appointment of proxies for the representative.

e) The technical prevention unit, explicitly stating, at least:

- The hierarchical position of this body in the subject party's organisation chart and to whom it reports.

- The prevention tasks allocated to it and the staff dedicated to each of these.

- The procedures applied in developing its functions, and the human and technical resources available to it.

- In the event that it performs other functions not directly related to PML/TF, state what these are and the extent of specific dedication to prevention work.

- Prevention unit staff must have an appropriate profile for the work they perform and be duly trained.

3.4. The responsibilities of directors and senior managers

a) State explicitly the responsibilities of those who exercise director or senior management roles in the subject party with regard to offences when these are wilful or due to negligent conduct.

3.5. Customer acceptance policy

a) The content, implementation and effective application of the customer acceptance policy. A list of the **customer categories** considered for prevention purposes, and the parameters for inclusion in these. A description of the profile of those customers with greater than average risk, and the **measures adopted and procedures established in this regard** (e.g. obtaining additional information and documentation,

the need for express authorisation for acceptance from a higher level body with competencies in this area, etc.).

The types of documents (identification and understanding) to be required from the highest risk customers must be clearly defined.

b) A classification of the customer base into each of the categories defined, based on analysis of ML/TF risks.

c) Any IT applications used for effective compliance with the customer acceptance policy and customer classification and segmentation.

3.6. Due diligence measures and their application

a) Customer identification procedures, expressly stating the types of documents to be obtained.

b) The procedures for understanding the customer's activity, expressly indicating the forms used for identifying and understanding the customer. The way that data on the customer's activities is processed and how this is used in preparing profiles and detecting and analysing any event or transaction that might be related to ML/TF.

Subject parties must keep a file, database, register, etc. for each of their customers (a **"know your customer" file**), detailing and centralising all information on the customer and the business relationships established, including that obtained from the due diligence measures corresponding to their risk levels.

c) The process for verifying activities declared by customers, expressly stating the types of documents to be requested, the stage at which they should be requested and the potential checks to carry out (using internal and external sources) to provide a reasonable assessment of the professional or business activity declared. The documents that must be received, for each customer type, **before the subject party can authorise the start of operations** with the customer.

d) The procedures in place to identify the actual beneficiary and to check their identity in the case of relationships with customers acting for third parties. The measures implemented to determine the ownership and control structure of legal persons.

e) The measures applied for continuous monitoring of the business relationship so as to ensure that the customer's transactions are consistent with the entity's understanding of the customer's activity and business and risk profile, being particularly sensitive to changes in customer behaviour. The measures put in place to ensure that documents, data and information are up-to-date, establishing reasonable periods for updating such resources for each customer category based on their risk profile.

Specific, enhanced monitoring of the customer's activity should be carried out during the initial months of the relationship with new customers, and for transactions involving new products and services not previously offered by the subject party, so as to ensure that the **transactions carried out match the entity's understanding** of its customers and their business and risk profiles.

f) Express measures to comply with the legal obligation not to establish business relations or carry out transactions when it is not possible to apply the due diligence measures set out in Act 10/2010, and to bring the business relationship to a close when

it is impossible to apply these measures during the ongoing business relationship. The need to keep an up-to-date **register** of customers with whom the business relationship has been brought to an end. This register must adequately identify these customers, providing a detailed description of the reasons for ending the business relationship.

g) As applicable, the possibility to turn to third parties subject to Act 10/2010 to apply the due diligence measures planned, with the exception of the continuous monitoring of the business relationship. The requirements and conditions for this, in particular, **a written agreement** between the subject party and the third party establishing their respective obligations.

h) As applicable, and pursuant to current regulations, exceptions to the obligation to apply certain due diligence measures with regard to particular customers, products or transactions. The need to keep a **register** of these.

i) Enhanced due diligence measures (e.g. obtaining or requesting additional information and documentation, express authorisation from a competent higher level body, etc.) for the highest risk business areas and activities, stipulating the content of these. Identification of the areas, customers and products, etc. considered to be the highest risk, covering, as appropriate, the following areas at least:

   - Private banking.
   - Cross-border banking counterparts.
   - Remote business relationships and transactions by telephone or electronic means.
   - Money transfer and foreign exchange services.
   - Other high-risk products and customers, such as persons with public responsibilities, high-risk geographic areas and others considered such by the subject party.
   - The types of risk transactions associated with certain activities or customers from countries considered high risk for prevention purposes.
   - New customers and transactions as set out in point 6.e) above.

3.7. Archiving customer and transaction documentation

a) The procedure established preserving documentation required in application of the due diligence measures and adequately documenting the transactions carried out, expressly indicating the period for retention and the start date for this period, together with the conservation medium for ensuring they remain in suitable condition, that they can be read correctly, can be found and can not be tampered with.

3.8. Systematic reporting of transactions

a) The procedure for systematic reporting to SEPBLAC (the DMO, or monthly transaction declaration), including, at least:

   - A list of transactions susceptible to being reported under current regulations.
   - The way of obtaining and capturing such transactions.

- The people, bodies and departments responsible for preparing such communications.
- The nature and operation of the IT applications used in the procedure.

b) The measures applied to detect possible division of transactions when preparing the monthly transaction declaration, expressly mentioning the nature and operation of the IT applications used in the detection procedure.

c) Any procedure in place for granting exceptions to customers from the monthly transaction declaration, expressly mentioning, at least:

- Prior approval from the internal control body.
- The criteria used in granting exceptions.
- The term of the exceptions.
- The need for written evidence of clients granted exceptions, and the justified reasons for such exceptions.

d) In the event that there are no transactions to be reported in a period, the procedure in place for a negative six-monthly communication to SEPBLAC.

e) The procedure for analysing the transactions included in the monthly declaration to identify any showing signs of being related to ML/TF, in which case they will also be reported to SEPBLAC.

f) The procedures established by the subject party for monthly communication to the Commission's Executive Service of any transactions in which they are involved that show signs of requiring mandatory declaration. As applicable, reporting the refusal of the subject party to show or present the declaration.

g) In the case of credit institutions, the measures in place to check and process the declaration forms for means of payment in the situations provided for in the regulations, and for sending the appropriate information to the Commission's Executive Service.

h) For subject parties involved in foreign exchange and international money transfers, if the customer fails to provide the documentation required, the transaction should be included, together with all information it has been possible to obtain on it, in the monthly transaction declaration to SEPBLAC. The criteria for detecting such transactions.

3.9. Detection and analysis of transactions that might be related to money laundering or terrorist financing

a) The **alert system or systems** used to detect any transactions that might, due to their nature (complexity, unusual nature, apparent legal or economic purpose, or because of signs or concealment or fraud), be related to ML/TF.

b) With regard to the specific procedure for detecting transactions related to terrorist financing, the procedure for consulting published international lists prior to establishing business relationships, and periodic checks of the entire customer base against these lists to take account of any updates. The procedure followed in the event of any matches on the list.

c) The IT application(s) used to detect transactions that might be related to ML/TF, as a minimum setting out:

- The persons, body or department responsible for managing and using these applications.
- The types of alerts set up and the characteristics of these, the risk thresholds defined, and the circuits put in place for dealing with different alerts, creating a trail of the work carried out.
- Alerts based on detection of transactions that do not match the subject party's understanding of their customer, and their business and risk profile.
- Access to the entity's other IT applications that might contain relevant information for prevention.
- The procedure for incorporating new risk variables into the alert system, in response to the entity's practical experience.

Irrespective of whether physically located or managed in Spain or abroad, the systems and applications used for prevention must meet current requirements under Spanish prevention regulations. All information and documentation generated by such systems and applications must be adequately **available and accessible** for the internal control purposes of the subject party in Spain, and to respond in good time and due form to any requirements from Spanish authorities.

d) The subject party must have in place responsive procedures for detecting and processing transactions that require **urgent** due diligence measures as they are due to be executed immediately.

e) The procedure for action in the event of alerts relating to the transactions of usual customers, for which the subject party is sufficiently aware of the legal nature of their activities. This knowledge of the activities carried out by the customer justifying the decision not to analyse an alert in greater detail must be duly recorded with appropriate documentation.

f) Subject parties must have a **catalogue or register of types of transactions** related to ML/TF, developed based on their activity and experience during the course of their business relationships. Each of the risk-transaction types must include and describe a **specific pattern and series of risk elements**, and the actions to be taken in the event of detecting signs of such transaction types; this will basically involve abstaining from executing the transaction and reporting it to SEPBLAC.

This catalogue or register of types of transactions must be regularly reviewed and fed with new information, based on the activity and experience of the subject parties during the course of their business relationships.

g) Further to the previous point, the manual shall include the establishment of a responsive reporting channel between the prevention bodies and business units, in relation to the types of transactions that should not be accepted or executed due to displaying previously-established patterns or signs of risks common to operations related to ML/TF. The procedure for communicating this catalogue or register of risk types to business units must ensure that they are capable of detecting and stopping the execution of transactions that match or show signs of such risk patterns before they occur.

h) In the event that prevention bodies detect the repeated execution of transactions that have been included in the catalogue or register of types of risk transactions, the communication channels and procedures between these bodies and the business units must be checked to ensure that they are **working correctly**, and an explanation must be sought for why the business units are continuing to accept and execute such transactions.

i) The internal procedure for reporting risk transactions by the staff and managers of the subject party to persons, bodies and departments responsible for prevention, expressly referring to at least:

- The internal form used for such reporting.
- The internal reporting channels established.
- The systems put in place for registering, monitoring and ensuring the confidentiality of the reports sent.
- The information sent to staff and managers about progress with reports they have submitted, specifying the schedule for action.

j) The **special analysis** procedure for those alerts at the greatest risk of being related to ML/TF. This should first spell out what is meant by special analysis, as opposed to initial or early analysis of internal alerts and communications received. This procedure should be performed referring, at least, to the following:

- The persons, body or department responsible for centralised analysis of the transactions detected. The opening of cases for each analysis undertaken.
- The internal and external databases and additional information sources consulted, etc.
- Use of appropriate IT applications to manage the special analysis, and the characteristics and operations of these applications.
- The procedure established for taking decisions in relation to filing or reporting to SEPBLAC transactions analysed, and the periods established for these. **Reasons must be given for the decision taken for each transaction** subject to special analysis, stating why it was decided to report, not report or continue to monitor the transaction. Likewise, **reasons must be given and explained** for any **decision to end a business relationship, in part or in full,** with any customer in one of the aforementioned cases.
- The reason for the decision to report, continue to monitor or file a transaction must be consistent with the analysis carried out; the case file must include the documentation considered necessary for the decision reached.

k) The procedure for **preparing reports and conclusions on each special analysis carried out**. Such reports must summarise the essence of the transaction and conform to a standard structure, describing step-by-step all related aspects, from start to finish, and reaching a conclusion consistent with the results of the analysis. The report must not merely describe the transaction carried out; it must focus on justifying the final decision taken (i.e. whether to report, continue monitoring or file the case).

l) With regard to adequate registering of those transactions subjected to special analysis, the subject parties will keep a **database or register of all transactions subject to special analysis**. This database will be used to register all the basic elements of all such transactions

(transaction class, amount, the date the relationship was established with the customer, customer nationality, sector, source and/or destination of funds, the risk indicator that triggered the alarm, etc.). The database should also include a reasoned explanation of the decision made in the particular case (report to SEPBLAC, continue monitoring, file).

m) The procedure established for processing and managing alerts, customers and transactions classified as "in monitoring" or similar (controls applied; obtain additional information; monitoring process; frequency of status review; any time limits for retaining a particular status; etc.).

3.10. Abstention from execution

The obligation to abstain from executing suspicious transactions is defined in Act 10/2010 as:

a) Refraining from establishing relationships or carrying out transactions when the subject parties can not apply the due diligence measures set out in Act 10/2010, or when the transaction presents clear indications of being related to ML/TF.

b) Terminating a business relationship when during its operation it becomes apparent that it is impossible to apply the due diligence measures set out in the Act, or when the transaction presents clear indications of being related to ML/TF, at which stage it shall be subject to special analysis.

c) And, more specifically, refraining from establishing or maintaining business relationships with legal persons whose ownership or control structure can not be determined.

In relation to this obligation, the manual should make express reference, at least, to:

- The procedure followed to ensure compliance with this obligation by the subject party, their employees and agents.

  In relation to the duty to abstain, the subject party must have in place responsive procedures for detecting and processing any transactions to which due diligence measures must be applied urgently, given that they are about to occur or be executed imminently.

- The person, body or department responsible for decision making and communicating to employees how they should act. Written justification, as appropriate, of the total or partial cancellation of the business relationship for causes or reasons related to PML/TF.

- Possible exceptions to this obligation and subsequent requirements in the event that such exceptions are applied. The procedure used in the event of **"return or reimbursement"** of funds received that, by applying the subject party's internal PML/TF policy, or because it is impossible to apply the due diligence measures set out in the Act (e.g. termination of the business relationship), must be returned to the customer. As far as possible, this procedure should be based on reimbursement of funds to the customer using the same payment media or instrument used to initially deposit the funds.

- Pursuant to section 3.9.g), a list of **specific communications or instructions** sent to business units about particular types of transactions that should not be accepted or executed as they show specific risk elements common to other transactions that have already been subject to special analysis and which show signs of being related to ML/TF. These communications or instructions must be set down in writing and **available at all times to SEPBLAC**.

- The **procedure established for full or partial severance of the customer relationship**, including the procedure for communicating this decision to the customer, taking account of the requirement for scrupulous compliance with the duty not to reveal communication of suspicious transactions to SEPBLAC.

3.11. Reporting of transactions that might be related to money laundering or terrorist financing

a) The procedure for reporting suspicious transactions to the Commission's Executive Service, expressly mentioning, at least:

   - The form used for such reporting.

   - The minimum content to be included in the communication under article 18.2 of Act 10/2010, clearly specifying the suspicious signs involved and **indicating the factor that provoked the report**.

   - Such reports must always include detailed information on all the measures taken to try to determine both the source of the funds and the real beneficiary of the transaction reported, even it is not possible to fully determine these.

   - The report must include a **description of the measures taken** in relation to the parties involved in the transaction reported (e.g. maintaining the business relationship without changes, cancelation, limits placed on the transaction, etc.), **justifying the reasons** if the relationship is continued. Such decisions must be made by the competent person, body or department in the subject party.

   - The reporting method implemented (electronic reporting in the case of credit institutions and written communication for other subject parties).

3.12. Compliance with the requirements of SEPBLAC and other authorities

a) The procedure established for responding to information requirements from the Executive Service and other authorities relating to PML/TF, expressly referring, at least, to:

   - The persons, body or department responsible for responding to the requirements received, and the means used for this.

   - In addition to all available information on the transactions requested and those involved in them, including in response to official requests **any other information related** to the transaction or those involved that the subject party considers relevant to a better understanding.

   - The procedure established to ensure that all PML/TF requirements received by the subject party should be made known to the persons or departments responsible for such prevention work; these parties must also keep a **register** of all the requirements received and the responses to them.

   - The subject party should assess the appropriateness or relevance of carrying out a special analysis of the customer involved in all information requirements or requests received from competent authorities.

3.13. Training

a) Subject parties must have a specific, ongoing PML/TF training policy, covering, at least:

- The design of an annual training plan, based on risks in the subject party's business sector. The annual plan must be approved by the internal control body.
- The basic content of the courses and material used, **including case studies of transactions with signs of ML/TF** or that might be specific to the sector in which the subject party operates.
- Duration and frequency.
- Form of training (in person or remote) and profile of trainers.
- The employees, departments and business areas at which the training is aimed, with courses being designed specifically for the profile of each group of employees.
- An initial PML/TF training course for new recruits.
- An evaluation system to assess the knowledge acquired from the courses.

3.14. Subsidiaries in Spain or abroad and branches

a) The control measures established by the subject party to ensure compliance with PML/TF regulations and internal procedures by Spanish subsidiaries.

b) Any procedure established by the subject party to ensure that its subsidiaries and branches abroad in which it has a majority holding have established and apply PML/TF procedures and measures in line with those established by the parent.

3.15. Agents and other intermediaries

a) Subject parties shall prepare a procedural manual applicable to their agents and other intermediaries, including the specific points relating to general internal regulations described in section 3.2, expressly indicating their scope of application and the form of distribution among such agents and intermediaries.

b) **Policy for contracting agents and other intermediaries**: establishment of specific requirements for contracting and the checks to be carried out on the profiles of candidates. These requirements and checks must include the application of suitable due diligence measures for the risk presented, specifying the body, department or post responsible for taking contracting decisions in each case.

In the event that the subject party's prevention bodies detect that any agent or intermediary, or any customers captured by such parties, are generating numerous ML/TF alerts, in addition to taking appropriate action for such cases (e.g. abstention from execution, termination of the business relationship, etc.), they must also review the effectiveness of their contracting policy.

c) **Control measures for agents and other intermediaries**. The need for special, enhanced monitoring of the activity of the agent or intermediary will be greater

during the initial phases of their activity with the subject party, in order to ensure that the transactions they are carrying out match the subject party's understanding of the agent or intermediary and their business and risk profile.

d) Training policy for agents and other intermediaries.

e) A summary of the PML/TF aspects to be included in contract clauses in agreements with agents and intermediaries.

3.16. Internal verification

a) The internal audit work undertaken to verify compliance with PML/TF obligations by the subject party and the effectiveness of the prevention system, specifically mentioning, at least:

- The audit plan with regard to prevention, covering the operations of the prevention unit and business networks, and the overall effectiveness of the prevention system.
- The persons, body or departments responsible for implementation.
- Specific aspects and content reviewed.
- The frequency of internal reviews.
- Whether carried out on site or remotely.
- Audits of subsidiaries and agents.
- The body informed of the results of such audits and the procedures established to ensure correction of weaknesses and deficiencies identified in a reasonable period.
- **An opinion on the degree of the subject party's compliance with these recommendations and that of the departments involved in its prevention system (business networks, prevention bodies, etc.)**
- Collection of samples to form an opinion on the effectiveness of the prevention system as a whole, including a sample of transactions subject to special analysis that were ultimately filed and not communicated to SEPBLAC, so as to check there is a duly reasoned case and documentation for this decision.

3.17. External expert review

a) The procedure established for hiring an external expert and checking their suitability.

b) **The subject party must ensure that the external expert reports expressly on the adequacy of its policies, procedures and manuals and the recommendations set out herein.**

c) The subject party shall ensure that the external expert examines the samples needed to support their opinion and the recommendations made in accordance with Order EHA 2444/2007, of 31 July. The object, selection procedure and results of these samples must be detailed in the report.

3.18. Other relevant aspects not covered above

a) Any other procedure, measure or information to prevent money laundering and terrorist financing considered relevant.