BANCO SABADELL GROUP ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY EXTRACT

This document is a translation of a Spanish language document which was approved by the Board of Directors of Banco de Sabadell, S.A. on 30/09/2021. The Spanish version of this document will prevail in the event of any discrepancy or dispute.

CONTENTS

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

1. Introduction

1.1. Definition

For the purposes of this Policy, the term **Money Laundering** shall be considered to refer to the following activities:

a) The conversion or transfer of assets, in the knowledge that those assets are the product of criminal activity or participation in a criminal activity, with the aim of concealing or covering up the illicit origin of those assets or to collaborate with any person involved to evade the legal consequences of their actions.

b) The act of concealing or covering up of the nature, origin, location, availability, movement or real ownership of assets or rights over assets, in the knowledge that those assets are the product of criminal activity or participation in a criminal activity.

c) The acquisition, possession or use of assets, in the knowledge, on receipt of such assets, that they are the product of criminal activity or participation in a criminal activity.

d) Participation in any of the activities mentioned in the points a), b) and c) hereinabove, association with another party or parties to commit these types of activities, attempts to perpetrate such activities and aiding, abetting or advising another party to commit such activities or facilitating their commission.

Money laundering shall exist even when the activities described in points a) to d) hereinabove are the result of negligence.

Similarly, money laundering shall exist even when the activities described in points a) to d) hereinabove are carried out by the person or persons who committed the criminal activity that produced the assets.

Assets that are the product of a criminal activity are understood as all types of assets whose acquisition or possession originates from a crime (both material as well as immaterial, assets or real estate, tangible or intangible) as well as legal documents or instruments regardless of their form, including electronic or digital, that accredit the ownership of those assets or a right thereto, including payment fraud in the case of crimes against the Public Treasury.

Money laundering shall be considered to exist even when the activities that produced the assets were carried out in the territory of a foreign State.

It shall be of greater concern when the assets are the product of a criminal activity related to drug trafficking or corruption.

****

Terrorism financing is understood to refer to the supply, deposit, distribution or collection of funds or property through any means, directly or indirectly, with the intention of using them or with the knowledge that they will be used, fully or partly, for the commission of any of the terrorist crimes categorised as such in the legislation in force at any time.

Terrorism financing shall be considered to exist even when the supply or collection of funds or property have been carried out in the territory of another State.

1.2. Purpose and unit responsible

Banco Sabadell Group (hereinafter, "the Group" or "BSab Group") has prepared this document, entitled "Anti-Money Laundering and Counter-Terrorism Financing Policy" (hereinafter, "the Policy") with the aim of establishing the principles, critical management parameters, governance structure, roles and functions, procedures, tools and controls applicable in relation to Anti-Money Laundering and Counter-Terrorist Financing (hereinafter, AML/CTF), in addition to providing details of the main procedures applicable to ensure that MLTF risks are identified and managed at all levels of the Group.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

The unit responsible for this Policy is the Compliance Division of Banco de Sabadell, S.A., due to its responsibility in defining general guidelines and in managing the Group's compliance function.

1.3. Scope of application

This Policy sets out the management and control model for the prevention of money laundering and terrorism financing and is applicable to all Group entities (hereinafter, "Entities"), which are subject to AML/CTF regulations and legislation as a result of their activity, in accordance with the provisions of the BANCO SABADELL GROUP'S GOVERNANCE POLICY FOR REGULATORY DOCUMENTS. Furthermore, compliance with the provisions of this Policy is mandatory for all employees, directors and members of the Governance and Management Bodies of Group entities.

The foregoing is irrespective of the requirement for compliance with other internal procedures that may be applicable to individual entities, depending on their activity or the region in which they are active.

1.4. Regulatory framework

The legal instruments used as a reference for this Policy shall be those applicable, in each case, depending on the type of entity and the region in which it is located. In any case, the regulatory framework applied in the Group's parent company shall be used as a reference for the entire Group, except in matters that have their own specific legislation due to the entity's activity or the region in which it is located.

Regulatory recommendations and guidelines must also be adhered to, in order to implement the best practices in this regard.

Also applicable is the Commission Delegated Regulation (EU) 2019-758 of 31 January 2019, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate MLTF risk in certain third countries.

In all cases, the management and oversight of compliance must be carried out in line with that set forth in the Banco Sabadell Group's Compliance Policy.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

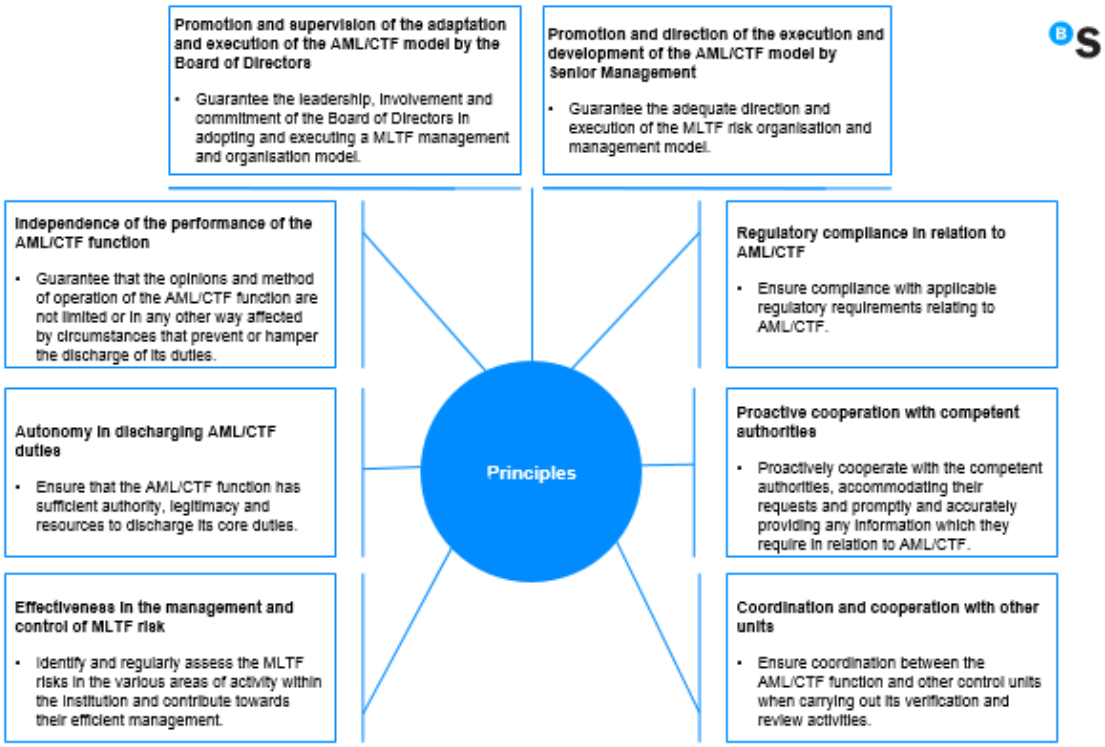
2. Basic principles and critical management parameters

The following principles and critical management parameters have been identified in relation to AML/CTF:

2.1. Principles

The figure below shows the principles of the ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY:

Figure 1. Principles of the Anti-Money Laundering and Counter-Terrorism Financing Policy



2.1.1. Promotion and supervision of the adaptation and execution of the AML/CTF management and control model by the Board of Directors

The Board of Directors of each entity, either directly or, where applicable, through the corresponding Committees, promotes and supervises the model for the organisation and management of MLTF risk of each Group entity. Their leadership, involvement and commitment form the foundation for the establishment of an effective AML/CTF model, so that money laundering and terrorism financing risk may be reduced.

Their main duties include setting strategies for the implementation of an effective AML/CTF model, the approval of the Policy, and facilitating the establishment of the necessary mechanisms and procedures for its implementation. Furthermore, they must ensure that the strategies, policies and procedures are adequate, effectively implemented and regularly reviewed, assigning sufficient resources for such purposes.

In this respect, the Board of Directors of the Group's parent company, Banco de Sabadell, S.A., designates the Internal Control Body (ICB) as the body tasked with the oversight and compliance of the AML/CTF model.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

2.1.2. Promotion and direction of the execution and development of the AML/CTF management and control model by Senior Management

In each Group company, Senior Management supervises, coordinates and outlines guidelines relating to the execution and development of the model for the implementation of controls and procedures.

2.1.3. Independence of the performance of the AML/CTF function

Each individual entity must ensure that the AML/CTF function is afforded the utmost independence, so that its powers of judgement and action manner are not compromised by any circumstances that could obstruct or hinder the performance of the functions and responsibilities assigned to it.

To this end, the following aspects shall be considered:

- The AML/CTF function, forming part of the Compliance function, should have a position within the organisational hierarchy that guarantees its independent action in order to prevent conflicts of interest with other units in each Entity.
- When exercising its duties, it should not be affected by business, economic or any other type of targets or objectives which could undermine its independence of judgement to suggest or recommend activities in line with the AML/CTF objectives.
- The remuneration and performance appraisals of the AML/CTF function shall neither largely depend on the results of the activities that it controls, nor shall they compromise its impartiality and objectiveness. They must be mainly based on the achievement of objectives and targets related to its duties and responsibilities.

2.1.4. Autonomy in the development of AML/CTF duties

Entities shall guarantee that the AML/CTF function has enough autonomy to discharge its primary duties. It shall be granted sufficient authority and legitimacy in order to gather information at any time, or access the records and documents required to discharge its core duties within each entity.

The AML/CTF function will also have sufficient and appropriate resources, both human and technical, to make it easier to carry out its responsibilities on an autonomous basis and guarantee that compliance risk is effectively managed.

2.1.5. Effectiveness in the management and control of MLTF risk

Each entity shall identify and regularly assess the MLTF risks in the various units and contribute towards their efficient management.

As such, they shall establish adequate and effective procedures to prevent, detect, correct and mitigate any risk arising from the breach of any obligations imposed by AML/CTF rules and standards applicable to each entity and, in particular, the risk of incurring sanctions, financial loss, material loss or loss to reputation as a result of an infringement of laws, regulations, rules and self-regulation standards applicable to their activities and the region in which they operate.

2.1.6. Regulatory compliance in relation to AML/CTF

The entities shall guarantee compliance with the regulatory requirements relating to the prevention of money laundering and terrorism financing that are applicable to them. They must also ensure that they adhere to regulatory recommendations and guidelines, in order to implement the best practices in this regard.

In all cases, the management and oversight of regulatory compliance must be carried out in line with the provisions of BANCO SABADELL GROUP'S COMPLIANCE POLICY.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

2.1.7. Proactive cooperation with the competent authorities in relation to AML/CTF

Entities must proactively cooperate with the competent authorities, accommodating their requests and promptly and accurately providing any information which they require to discharge their duties with regard to the prevention of money laundering and terrorism financing.

In particular, they must provide complete and diligent responses to any requests for information received from competent authorities within the established timeframe and in the requested manner, and they must guarantee transparency and provide the competent authorities with access to information to enable them to discharge their duties.

2.1.8. Coordination and cooperation with other units

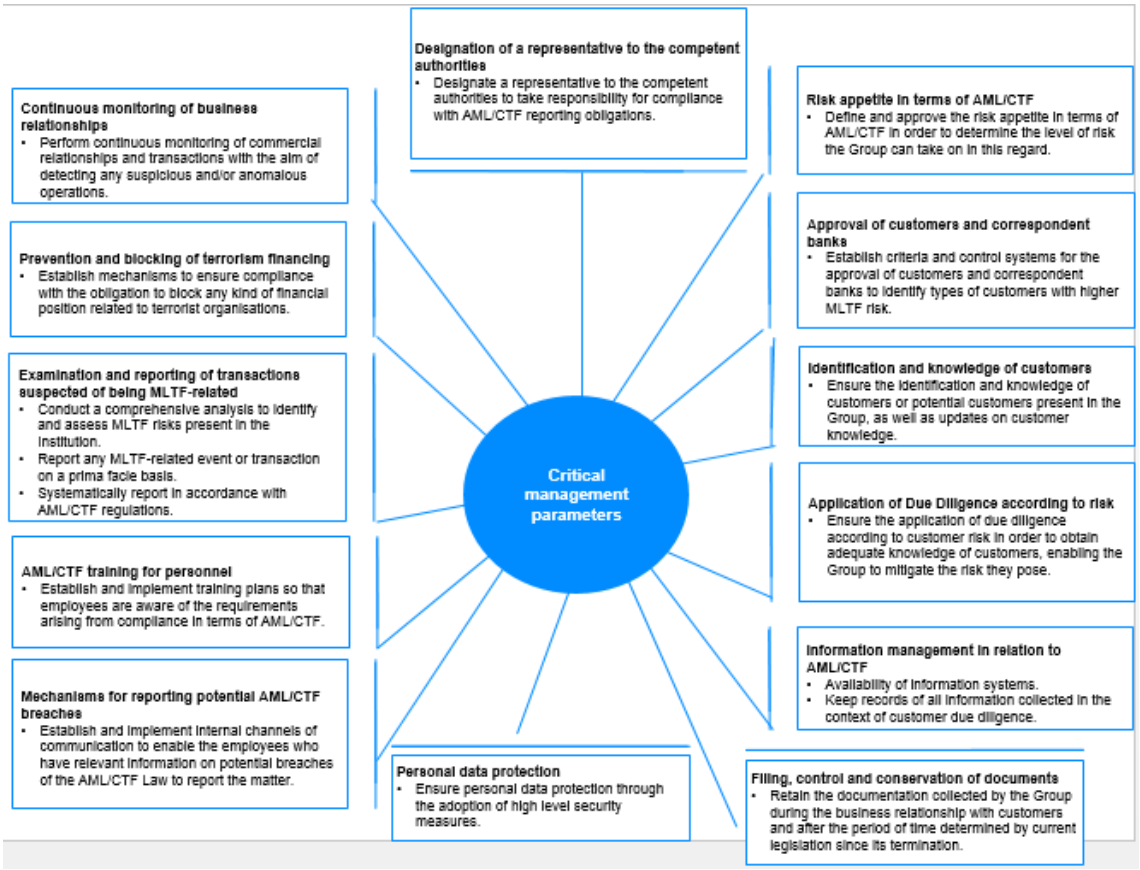
The AML/CTF function shall coordinate with other control units when carrying out its verification and review activities, in order for these units to provide each other with the necessary information to adequately supervise and control money laundering and terrorism financing risk whilst always respecting each other's scopes of work and independence.

The AML/CTF function may also request the support of other units when necessary given the nature of the information required, in order to carry out aspects relating to verification, control of operations or other similar aspects.

2.2. Critical management parameters

The figure below shows the critical management parameters for the ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY, always on the basis of the activity and region and applying the proportionality principle:

Figure 2. Critical management parameters for the Prevention of Money Laundering and Terrorism Financing



Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

2.2.1. Designation of a representative to the competent authorities

In accordance with the legal regulations in force in each jurisdiction, each Group entity must designate as its representative to the competent authorities a person who is either on the Board or performs a managerial function and who is responsible for compliance with the mandatory reporting requirements set out in the Spanish AML/CTF Law (Law 10/2010 of 28 April on the prevention of money laundering and terrorism financing).

One of their main responsibilities is to report at regular intervals to the Institution's Board of Directors and to its Senior Management about the supervision of effective compliance with obligations in relation to AML/CTF.

The representative of Banco de Sabadell, S.A. to SEPBLAC (the Spanish Financial Intelligence Unit [*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*]), shall also be the representative of the Spanish entities that are bound by the obligations of the aforesaid AML/CTF Law, also referred to as the "obliged subjects".

The designated representative must also have access to the necessary material, technical and human resources and have unlimited access to all of the information held by the Institution in order to be able to correctly discharge his/her duties.

2.2.2. Risk tolerance framework established in relation to AML/CTF

Risk Self-Assessment Report

All Group entities must prepare, at regular intervals, a Risk Self-Assessment Report to enable an understanding of the risks assumed with regard to AML/CTF.

This Risk Self-Assessment Report must make it possible to identify the level of risk to which the entity is exposed and shall serve as the basis for the customisation of procedures or Manuals developed locally in relation to AML/CTF.

Segmentation by customer risk and transactions

Risks inherent to MLTF may be managed more efficiently and effectively if there is prior knowledge of the potential risk associated with different types of customers and their transactions, including credit transactions. In this respect, all the Group entities must design a procedure that enables segmentation according to different levels of MLTF risk.

The allocation of risk levels must be carried out based on a series of factors that should indicate the degree of potential danger posed by the customer or by their transactions.

The risk rating of each customer shall be constantly updated in line with the continuous monitoring of the business relationship.

The customer risk-rating shall reveal, at all times, the extent to which Due Diligence is applied, the frequency of customer record updates and the need to apply enhanced monitoring measures with regard to their transactions.

In the context of the Group's risk tolerance, the entities must also take into account proscribed customers and those that require prior authorisation by the AML/CTF Technical Areas or by other higher-level divisions.

2.2.3. Approval of customers and correspondent institutions

The entities must establish criteria and develop systems to control the procedures for the approval of customers and correspondent institutions, in order to facilitate the identification of the types of customers or correspondent institutions that are likely to pose a greater MLTF risk according to risk assessments carried out.

Those criteria and systems must include, among other things, the following content:

- List of the categories of customer or correspondent institutions for the purposes of AML/CTF and the criteria for inclusion in each category.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

- Description of the profile of customers and correspondent institutions that present a higher risk than average and the measures taken or action procedures established with regard to those risks.
- Risk stratification of customers and correspondent institutions based on a prior assessment of the risk associated with each one.
- IT applications used for the effective compliance of the procedure for the approval of customers and correspondent institutions, as well as their stratification or segmentation.

In all cases, the criteria for the approval of customers and correspondent institutions associated with activities in the arms industry must comply with the stipulations of the GROUP'S POLICY ON RESTRICTIONS ON FINANCING AND INVESTMENT IN THE ARMS INDUSTRY.

Furthermore, for reasons related to MLTF risk control, the Group shall not accept customers or correspondent institutions that fall into any of the following categories:

- Persons included in any public list related to terrorism or related groups.
- Persons or entities which have a record of being related to any kind of criminal activity.
- Persons or entities whose business dealings are such that it is impossible to verify the legitimacy of their activities or the source of their incoming funds.
- Business relationships shall not be established or maintained with legal persons or vehicles with an indeterminate shareholding or control structure.
- Persons or entities that refuse to provide the required information or documentation.
- Any entity or organisation that, by law, must have some form of administrative authorisation to operate but do not have it.
- Financial institutions with no physical presence (shell banks) in the region where they carry out their business and that do not belong to a regulated financial group.
- Financial institutions which, either directly through VOSTRO accounts or indirectly through a subaccount, enable the execution of transactions for customers of other credit institutions (payable-through account).
- Financial institutions that do not comply with FATCA regulations, unless there is no alternative entity in their country that does comply with those requirements.
- Correspondent institutions subject to blocks imposed by international organisations to which Spanish legislation must comply with.
- Correspondent institutions not subject to inspection by the licensing banking or regulatory authority.
- Correspondent institutions located in jurisdictions with full prohibition to operate by decision of the Internal Control Body through its Delegated Committee.
- Activities related to the provision of sex services (brothels, hostess clubs, etc.).
- Associations or similar organisations related to the consumption of narcotic substances or similar drugs (cannabis clubs, etc.).
- Persons who have been the subject of a special MLTF investigation and have had their account terminated and who, in a subsequent request to open an account reveal signs of ML or TF or provide information that is insufficient to apply reinforced due diligence measures.

Finally, the entities must establish controls to obtain prior authorisation for the approval of customers or correspondent institutions classified as high risk in terms of money laundering or terrorism financing, from the AML/CTF Technical Areas or from a higher level of Management.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

2.2.4. Identification and knowledge of customers

The fundamental imperative in the fight against the use of the financial system for money laundering and terrorism financing is the identification and knowledge of customers, whether regular or not, and of beneficial owners.

All Group entities must develop standards, procedures and internal controls focused on gaining effective and comprehensive knowledge of their customers and their activities, with the aim of:

- Confirming and documenting the true identity of customers who have any kind of commercial relationship with them. For those Group companies that allow remote registrations of customers, enhanced due diligence measures are applied to ensure customer identification.
- Confirming and documenting any additional information about the customer, in accordance with the corresponding MLTF risk assessment.
- Ensuring that no transactions are performed with individuals or entities whose identities cannot be confirmed, or who have not provided the requisite information, or who have provided false information or information with significant discrepancies that cannot be explained.

In addition, as established under the applicable regulations, when there are signs or certain knowledge that a customer is not acting on his/her own behalf, specific information will be gathered in order to establish the identity of the person(s) on whose behalf the customer acts.

2.2.5. Application of Due Diligence according to risk

Following formal identification and as described hereinabove, prior to customer registration, potential customers are classified according to the potential MLTF risk that they represent, resulting in Low, Medium or High Risk customers.

In addition, and having successfully completed the detailed approval procedure, customers are subject to Due Diligence Measures according to their corresponding level of risk, with the aim of gaining adequate knowledge of customer risk, thereby enabling the Group to mitigate the risk posed by individual customers.

In this respect, the entities must set up and implement the Due Diligence Measures specified in the prevailing AML/CTF legislation and regulations, and must ensure their correct application in practice.

Depending on the level of risk posed by customers, they will be the subject of Simplified, Standard or Enhanced Due Diligence Measures. These Measures must appear in each entity's AML/CTF procedures and may be augmented in accordance with the provisions of the prevailing legislation applicable to each Group entity.

In addition, the entities must ensure the regular updating of documentation, data and information obtained in the application of due diligence measures to all customers, with those classified as high risk being updated at least annually.

Each of Banco Sabadell Group entities, in accordance with current legal regulations in each jurisdiction, has controls in place that enable the identification, regular review and monitoring of persons with public responsibilities, their family members and close associates.

2.2.6. Information management in relation to AML/CTF

Availability of information systems

Each entity must have information systems to carry out continuous monitoring of all commercial relationships and transactions with their customers, thereby facilitating the detection of any anomalous or suspicious transactions or patterns of activity.

Entities must also ensure that they have integrated information management systems capable of providing, in timely fashion, the information required to identify, analyse and perform effective monitoring of their customers transactions. In this respect, the systems used and the information available must facilitate the task of monitoring customer relationships and must include all

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

information available about the relationship with the customer, including transaction history, documentation omitted during account opening and any significant changes in the customer's conduct or business profile, as well as any irregular transactions carried out through a customer account.

Record keeping

Each entity must establish procedures to ensure that a record is kept of all information collected in the context of customer due diligence and in relation to customers' individual transactions. Among other things, this includes:

- Keeping a record of documents submitted to the entity to verify the identity of a customer or effective beneficiary.
- Copying the relevant information contained in the aforesaid documents, or obtained by other means, into the entity's own IT systems.
- Keeping a record of all documentation on the assessment process related to the analysis and continuous monitoring of customers and their transactions, as well as the main conclusions drawn therefrom.

2.2.7. Filing, control and conservation of documents

Unless the corresponding local legislation makes provision for a longer period, the documentation, information and records must be kept for a period of 10 years, as from the date of account closure, or upon completion of the corresponding transaction or operation. Certain documents must be retained for use in any investigation or analysis with regard to possible cases of MLTF, including the following:

- Copies of the documents required for the performance of due diligence measures.
- Originals, or copies with probative value, of documents or records that duly certify transactions, the parties thereto and their business relationships.

In any case, each entity must store copies of formal customer identification documents in optical, magnetic or electronic storage media that can safeguard the integrity of the documents, enable correct reading of the data contained therein, prevent their manipulation and ensure their satisfactory conservation and location, in compliance with the corresponding access restrictions established under the specific legislation in each region.

In this respect, the obliged subjects must have a filing system that ensures the appropriate management and availability of the documentation, for the purposes of internal control and to enable a prompt and proper response to requests from the authorities.

The filing of documentation must comply with the data protection regulations in force.

2.2.8. Continuous monitoring of business relationships

The entities must perform continuous monitoring of all of their customers' commercial relationships and transactions with the aim of detecting any suspicious and/or anomalous operations that are at odds with the usual patterns of their banking activity.

In particular, any event or operation, regardless of its amount, which by its nature may be related to money laundering or terrorism financing, must be identified and analysed in detail.

In addition, any operation or behavioural pattern that presents as complex, unusual or with no apparent economic or lawful purpose, or that signals deceit or fraud, must be examined particularly carefully.

In this respect, Group entities must have procedures in place to ensure that customer activities that appear suspicious are examined immediately to establish the origin of the funds and the grounds for such activity and, if it is indeed found to be suspicious, to take appropriate action and inform the authorities in accordance with the applicable legislation.

In addition, Group entities must have procedures in place to enable the establishment of an alert system or automatic blocks with regard to the execution of transactions with natural or legal persons

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

or countries that are subject to sanctions or restrictions adopted by various international bodies (including the European Union and the United Nations Security Council) in their respective programmes or lists of sanctions against specific countries, natural or legal persons, or entities that represent a threat to international peace and security.

Abstention from transaction execution

Provided the regulations in force so permit, Group entities shall abstain from carrying out any transaction where there are suspicions or certainty of its link to money laundering and terrorism financing. Similarly, transactions shall not be executed if they show a substantial lack of consistency in terms of the nature and volume of the activity or customers' operating history, or if there is no observable economic, professional or business justification to support the execution of such transaction.

Duty of confidentiality and ban on disclosure

Group entities shall adopt appropriate measures to maintain confidentiality concerning the identity of employees who have reported a potential irregularity to the internal control bodies.

Employees are strictly prohibited from disclosing to any customer or third party, with the exception of the particular persons or bodies designated internally and the competent authorities, the fact that information concerning AML/CTF has been reported or that an investigation is or may be underway into any operation that may be related to money laundering or terrorism financing.

2.2.9. Prevention and blocking of terrorism financing

With the aim of preventing terrorism financing activities, Group entities must establish procedures to enable the blocking of accounts, balances and financial positions, as well as transactions and capital flows, even those that appear intermittent, and their corresponding collection, payment or transfer operations, in which the ordering party, issuer, holder, beneficiary or recipient is a person or entity linked to terrorist groups or organisations or when the transaction, capital flow or operation has been performed with the purpose of, or in connection with, the perpetration of terrorist activities, or to contribute to the objectives pursued by terrorist groups or organisations.

In this respect, the entities must establish appropriate and effective mechanisms to ensure compliance with the obligation to block any kind of financial position related to terrorist organisations, thereby preventing it from being used or channelled into terrorist actions.

2.2.10. Examination and reporting of transactions suspected of being MLTF-related

Examination of transactions suspected of being MLTF-related

The entities shall have standards and procedures that establish the obligation to carry out an examination and investigation of customers/transactions identified as being potentially linked to money laundering or terrorism financing.

Appropriate due diligence measures and their corresponding checks must be carried out during the examination process, with the aim of determining the veracity of the information and to certify the identity, activity, origin and destination of funds and the consistency of the transaction history.

The examination shall cover all parties concerned in the transaction history under analysis.

Reporting of transactions suspected of being MLTF-related

The entities must establish procedures that make provision for the immediate recording and reporting of suspicious transactions to their internal AML/CTF bodies, so that they, in accordance with local legislation, carry out the necessary checks and submit the appropriate reports or notices of suspicious operations to the relevant authorities.

When Group entities or employees report information concerning suspicious operations or activity to the internal AML/CTF bodies, following the procedure set out in internal regulations, they shall be strictly prohibited from disclosing any information about the customers or operations set out in such communications.

Disclaimer of liability

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

Without prejudice to the local legislation of each Group entity that may expressly govern in this respect, it shall be understood that when the entities or, exceptionally, their managers or employees report information to the competent authorities in good faith, this shall not constitute a breach of the restrictions on information disclosure imposed either contractually or by any legal or regulatory provision, and shall not entail any form of liability on the part of the obliged subjects, their managers or employees.

2.2.11. AML/CTF training for personnel

The entities must make it a priority to adopt the necessary measures to ensure that all employees receive ongoing training around the requirements arising from AML/CTF legislation and regulations.

Training plans must be established and implemented so that employees are aware of the requirements arising from compliance in terms of AML/CTF, and these plans shall be approved by the internal control bodies.

In particular, employees should be given specific training oriented towards the pre-emptive detection, examination and reporting of customers or operations that may be related to money laundering or terrorism financing and they should be taught how to proceed in such cases.

Similarly, the scope and frequency of the training must be adapted to the risk factors to which employees are exposed as a result of their duties and responsibilities, and to the level and type of risk faced by the entity.

The training programmes shall take into consideration the international rules and local legislation related to MLTF, the latest trends exhibited in these criminal activities, and the Group's standards and procedures to combat MLTF, including how to recognise and report suspicious activities.

Apart from the general training programmes, all AML/CTF officers of the entities must keep themselves fully informed and must pass on information, on an ongoing basis, to the employees who report to them, concerning all regulatory amendments in this regard, as well as any new methods, techniques or procedures discovered that may be used for money laundering or terrorism financing.

2.2.12. Mechanisms for reporting potential AML/CTF breaches

The entities must establish internal communication channels, which must be properly publicised internally, to enable employees who have relevant information about potential breaches of the AML/CTF Law, its implementing rules or the policies and procedures introduced to comply with the aforesaid, committed within the Bank, Group subsidiaries and/or foreign branches, to report such information, even anonymously.

Those procedures must include the obligations of the bodies designated in that regard to examine and resolve such reported matters.

In addition, the provisions of personal data protection legislation shall apply to this system and procedure and ensure that the employee reporting the possible breach is protected against retaliation, discrimination and any other unfair treatment.

2.2.13. Personal data protection

The processing of personal data, as well as the files created to comply with the provisions of AML/CTF regulations, shall be carried out in compliance with the corresponding local legislation with regard to data protection. In all cases, high-level security measures must be adopted when dealing with such files.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

3. Procedures

Each Group entity shall prepare internal procedures and/or manuals that give a detailed description of the implementation, development and application of the established AML/CTF model.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

4. Tools

In a manner commensurate to each entity's level of activity and the degree of its exposure to the risks to which this Policy refers, Group entities must acquire and implement the tools, controls and procedures required for sound management of the AML/CTF model so as to ensure control of the following applicable matters:

- Assignment of MLTF risk to customers so that different levels of due diligence may be applied, both during customer registration and throughout the continuous monitoring of the business relationship.
- Identification of customers, parties and beneficial owners.
- Detection via automated tracking system of suspicious operations.
- Detection via automated tracking system of persons, parties and countries involved in transactions that may be included in lists related to terrorism and international sanctions.
- Risk indicators to monitor MLTF risk on an ongoing basis.
- Programme to oversee and maintain the AML/CTF model.
- MetricStream GRC or similar technology. These are tools that allow the management of compliance risks (including MLTF risk) to be automated, including control programmes, risk maps and controls, record-keeping and storage of documentary proof and reporting.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

5. Policy control

5.1. Control system

Compliance must carry out an Annual Supervision and Control Plan to comply with that set forth in this Policy.

5.2. Monitoring mechanisms

The results of these control programmes must be reported in line with the established requirements, enabling the results obtained and the applicable corrective measures, if any, to be adequately monitored by the governing bodies of each Group entity. These reports include, among others:

- Risk Self-Assessment Report on money laundering and terrorism financing.
- If applicable, an annual report prepared by an external expert in relation to the Prevention of Money Laundering and Terrorism Financing, which will be submitted to the Governance and Management Bodies, and to the Board of Directors.
- Ad-hoc reports submitted to the Management Body in the event that a significant MLTF risk is detected.

In addition, the Compliance Division of each Group entity must inform the Compliance Division of the parent company of any matters that, given their level of importance, may have an impact at Group level, including those set out in the following paragraph.

Appropriate precautions shall be established for the transfer of the aforesaid information and documentation with regard to the use of information transferred via the communication systems that the Group companies may have installed at any time.

5.3. Alerts

Each Group company will establish risk indicators relating to this matter, with a range of alert levels.

Compliance will include this information in its various reports, including its monthly reports on Operational Risk systems.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

6. Document governance

6.1. Document approval

This Group Policy is approved by the Board of Directors of Banco Sabadell, S.A., as parent company of the Group.

6.2. Validity, amendments, reviews and exceptions

This Policy shall enter into effect on the date of its approval by the Board of Directors of Banco de Sabadell, S.A.

It must be reviewed by Compliance at least once a year, specifically to reassess its general structure and content.

This Policy shall also be reviewed when certain circumstances arise, including but not limited to:

- Changes in the regulatory framework and/or the supervisor's recommendations.
- Changes in the organisational and governance structure of the Compliance Division, its duties or the definition of its general guidelines relating to the Prevention of Money Laundering and Terrorism Financing, and any other matters which could potentially affect this activity.
- Changes to the organisational structure and general governance model of the Group related to this Policy.
- Changes in the business objectives and strategy or management approach linked to the Policy.
- Development of new policies or amendments to existing policies which impact this Policy.
- Substantial changes in any procedures related to this Policy.
- When the results of monitoring and control activities make it advisable to change certain actions in order to increase the level of compliance or reduce the impacts of such activities on the Group or its employees.

Any division within the Group may propose changes to the Policy. Any proposed changes shall be made following the guidelines set forth in the BANCO SABADELL'S GOVERNANCE POLICY FOR REGULATORY DOCUMENTS, as indicated hereafter:

- The Division responsible for the Policy, as policy owner, shall coordinate the assessment work and evaluate the suitability of the changes, amendments and/or adjustments proposed by any division.
- The Division responsible for the Policy shall submit the proposed aspects to be changed and the corresponding justification for such changes to the Policies Forum.
- The Policies Forum shall decide whether or not to accept the changes.
- The Division responsible for the Policy shall make the necessary adjustments to ensure that the new version follows the Group's validation and approval process.

6.3. Policy publication

This Policy is available to all Group employees through CanalBS or through any other channel deemed appropriate by the Bank at any time.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

7. Annexes

Annex 1: Change history

Version	Unit responsible	Date approved	Description
1	Anti-Money Laundering and Counter-Terrorist Financing	24/10/2019	
2	Anti-Money Laundering and Counter-Terrorist Financing	23/10/2020	Annual review
3	Anti-Money Laundering and Counter-Terrorist Financing	30/09/2021	Adaptation to regulatory changes introduced in Royal Decree Law 7/2021

Annex 2: Glossary of abbreviations and acronyms

Abbreviation / Acronym	Meaning
BSab	Banco Sabadell
AML/CTF	Anti-Money Laundering and Counter-Terrorism Financing
MLTF	Money Laundering and Terrorism Financing
CD	Compliance (Division)
ICD	Internal Control (Division)
LoD	Line of Defence
ICB	Internal Control Body
SEPBLAC	*Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales* (the Spanish Financial Intelligence Unit)
EU	European Union

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.

Confidential. Its dissemination is prohibited without the written consent of Banco de Sabadell, S.A.