

**ANTI-MONEY LAUNDERING AND  
COUNTERING TERRORISM FINANCING  
CORPORATE FRAMEWORK**

**FINAL VERSION: JULY 2017**

**TABLE OF CONTENTS**

- 1) Introduction**
- 2) Definition and scope**
- 3) Scope of application and implementation by subsidiaries**
- 4) Principles**
- 5) Roles and responsibilities**
- 6) Key processes**
- 7) Governance**
- 8) Ownership**
- 9) Validity Date and Periodic Review**

**Appendix: Definition of terms**

## 1) INTRODUCTION

The purpose of this framework is (i) to establish the principles and standards that must be adhered by entities of Santander Group (the "Group") in relation to the prevention and control of money laundering and terrorist financing ("AML/CTF"), and also for the purposes of compliance with international sanction programmes, (ii) to define roles and responsibilities in this area, (iii) to establish the policies and procedures that must be undertaken by Group entities and (iv) to define the essential features of the governance.

## 2) DEFINITION AND SCOPE

The following definitions are established for the purposes of this framework:

- **Money laundering:** Participation in any activity that has the aim of acquiring, possessing, controlling, using, converting, transferring, concealing or disguising the nature, source, location, disposition, movement or rights with respect to, or ownership of, criminal property in the knowledge that that property is the proceeds of criminal activity or participation in such activity.
- **Terrorist financing:** The provision, deposit, distribution or collection of any property, in any means, directly or indirectly, with the intention that the property be used, or knowing that the property will be used, in whole or in part, to commit a terrorist act.
- **International sanction programmes:** Instruments of a political, diplomatic and economic nature used by international institutions and countries to exert influence in areas such as the prevention and pursuit of terrorism, support and defence of human rights and civil liberties, deterrence of possible armed conflicts or the prohibition of the development of weapons of mass destruction.

Money laundering and terrorist financing are universal globalised phenomena that take advantage of the international economy and the gradual elimination of barriers to trade globally, calling for a coordinated global response by the international community and the financial sector to prevent the sector being used for illicit purposes. Santander recognises the importance of the fight against money laundering and terrorist financing as it affects essential aspects of social life. The Group will always fully cooperate with the relevant authorities in this area.

This framework should be read in conjunction with other Corporate Frameworks and, in particular, the provisions of the General Compliance & Conduct Framework, the internal regulation for operational risks and others related to outsourcing and agreements with third parties.

## 3) SCOPE OF APPLICATION AND APPLICATION TO SUBSIDIARIES

This Framework:

- is applicable throughout the whole Group, is applied on a mandatory basis and compliance with it must be evidenced.

- shall be adopted by the Board of Directors of entities subject to the Group Subsidiary Governance Model (GSGM).
- shall be adhered to by all entities within the Group with any adaptations being strictly limited to those required by local law and regulation. Any adaptation or waiver for any part of this framework must be limited to those required by local law and regulation and submitted to the Corporation for consideration and approval.
- includes reference to specific elements for local implementation all of which should be submitted to the Corporation for validation to ensure they are consistent with this Framework. These should also be subject to periodic review and updates.

#### 4) PRINCIPLES

The following principles reflect the minimum Group expectations of the Group as a whole. These principles are mandatory and must be applied at all times.

- **Assessment and management of business risk:** All Group entities will be classified by levels of risk for the purposes of designing and implementing measures and controls to mitigate such risks, and for applying greater supervision to high-risk areas of business, products and channels. This acknowledges that the risk of involvement in money laundering or terrorist financing is directly related to the type of business carried on by Group entities, the products they distribute, and the channels used. It also considers that this threat may be managed more efficiently if there is prior knowledge of the potential risk concerning the various types of business and products.
- **Customer risk segmentation, Identification and Know Your Customer:** Customers of subsidiaries of the Group must be classified by risk level for the purposes of designing and implementing measures and controls to mitigate these risks, and for applying greater control over high-risk customers and transactions. This acknowledges that the risks inherent to money laundering may be managed more efficiently if there is prior knowledge of the potential risk concerning the various types of customers and transactions.

Customers and transactions must be monitored on a continuous basis once such customers have established a formal relationship with a particular Santander entity.

Know Your Customer obligations to identify (and know your customer and their activities) must be established by appropriate due diligence. This obligation will be met in accordance with the provisions made by the applicable legislation and the risk level in areas of business, activities, products, services, distribution or sales channels, countries of operation and transactions carried out.

- **Prohibited customers or customers with enhanced acceptance measures:** Santander Group will not accept customers where the necessary data is not available, or which fall into one of the Group agreed categories of prohibited customers. Prohibited customers are as follows:

- Persons on official sanctioned lists or persons that are related to<sup>1</sup> countries prohibited by the Group in the terms determined.
- Persons where information is available to suggest that they may be involved in criminal activities.
- Persons with businesses the nature of which makes it impossible to verify the legitimacy of the activities or the origin of the funds.
- Persons who refuse to provide the information or documentation required.
- Legal entities where the shareholder structure or control structure cannot be determined.
- Casinos or gambling companies that are not officially authorised.
- Financial institutions that are registered in countries or territories in which they do not have a physical presence (also known as "shell banks").
- Customers on the list of prohibited customers in the Santander Group's corporate policies.

The following categories of customers will only be accepted with prior authorisation by the internal governance body responsible for anti- money laundering and financing of terrorism<sup>2</sup>:

- Customers involved with the production or distribution of weapons and other military products.
  - Casinos or gambling companies officially authorised.
  - Foreign exchange companies, money transmission companies or similar.
  - Politically exposed persons (PEPs<sup>3</sup>) and their and their relatives and close associates<sup>4</sup>.
- **Transaction monitoring and analysis:** Ongoing monitoring of a business relationship with all types of customers must be conducted, controlling and analysing sensitive or high-risk transactions in connection with money laundering and terrorist financing, in order to detect suspicious transactions.

Proper IT systems must be available to this end, taking into consideration the type of transactions, business sector, geographic environment and transactional volume.

Enhanced monitoring must be applied to material high-risk customers and transactions, taking into account the key indicators for these customers and their accounts, considering circumstances as countries of origin, the origin of funds, the type of transactions and other risk factors.

---

<sup>1</sup> That have a link to the prohibited country or to individuals or legal entities resident or incorporated in the prohibited country, or are related to the government or the official institutions of the state (even if they are resident outside the prohibited country).

<sup>2</sup> The most senior management committee in relation to AML/CTF.

<sup>3</sup> PEP is an individual who is, or has at any point in the preceding years, been entrusted with a prominent public function. A 'prominent public function' may include but is not limited to: Heads of State; Heads of Government and Ministers (including deputy and assistant ministers); Members of Parliament (or of similar legislative bodies); and senior officials of major political parties; Senior Judicial Officials; Central bank board members; Ambassadors and high-ranking armed forces officials; Members of ruling Royal families with governance responsibilities; Senior Executives of state-owned enterprises; and Directors, deputy directors and members of the board or equivalent function of an international organisation

<sup>4</sup> a) a spouse (including a person who is considered by national law to be equivalent to a spouse; b) a partner; c) children and their spouses or partners; d) siblings and e) parents (including in-laws where this can be ascertained).

'Known close associates' include: a) A person who is a joint beneficial owner of a legal entity (or other arrangement) with a PEP; b) A person who is a close business relation of a PEP; and c) A person who is the sole beneficial owner of an arrangement set up for the benefit of a PEP.

- **Suspicious transaction reporting and systematic reporting:** Group entities must fulfil the obligation of reporting and cooperate with the relevant authorities.

Group entities must ensure that all employees are aware of their obligations to immediately report potentially suspicious transactions to the internal AML/CTF unit, in order to, in accordance with the law, make the necessary review and report or notification of suspicious transactions to the authorities.

Group entities must ensure that all employees are aware of their obligations when reporting a potentially suspicious transaction or activity to the internal AML/CTF unit, including not to provide any information, internally or externally, on concerned customers or transactions.

Group entities must ensure that the blocking of transactions and movement of funds and/or the prohibition of opening accounts is executed in line with local law and regulation.

- **Record-keeping:** Group entities must ensure that robust record-keeping is maintained and that, as a minimum, documents listed are kept for a period of at least six years or any longer periods that applicable local law or regulation dictates:
  - Documentation regarding identifying and knowing your customers.
  - Reports submitted to the authorities concerning the suspicious activities of a customer in connection with potential money laundering and/or terrorist financing, along with any supporting documentation.
  - Registers of training on money laundering and terrorist financing.
  - Any other documents or registers that must be kept by applicable legislation of anti-money laundering or terrorist financing.
- **AML/CTF Training:** All employees must receive ongoing training on the obligations arising from regulations on the anti-money laundering and terrorist financing. This must be facilitated through:
  - Annual training plans and targeted training to managers and employees and specifically staff performing those jobs that, by nature, are suitable for detecting any events or transactions that may be related to money laundering or terrorist financing, enable the employees to carry out detection and know how to proceed in such cases.
  - Ensuring that training plans and programmes determine the staff who require targeted training for the purposes of assessing the risk of money laundering and terrorist financing inherent to their functions or roles.
  - The registration of all training, with a description of the main characteristics and contents.
  - Continual sharing of information to all those responsible for anti-money laundering in all business entities of any regulatory changes in this area, as well as any new systems, techniques or procedures detected that may be used for money laundering or terrorist financing.
- **Sanction programmes:** Group entities must have effective policies and procedures in place in order to effectively comply with the restrictions under sanction programmes and international financial countermeasures.

Group entities must identify and follow sanction programmes and financial countermeasures, monitor the international sanction programmes issued by UN, EU and OFAC that might affect the activities of the Santander Group.

Group entities must risk assess and manage to determine the extent to which a business relationship or activity may be affected by international restrictions, and approach must be taken into account in risk assessment methodology.

Group entities must refrain from conducting business relationships with restricted persons and entities. No direct or indirect relations shall be established with persons and entities subject to international restrictions. To this end, appropriate and up to date knowledge of customers, their activity, and other persons and entities carrying on relationships with the Group should be obtained.

Group entities must maintain commercial operations and payments in compliance with restrictions. Transactions carried out by Group entities must be compliant with the restrictions under international sanction programmes, and no transactions can be undertaken if they fail to meet the conditions set out in the programmes.

Group entities must block assets when required. There must be means to detect relations with persons or transactions which do not comply with sanctions programmes. There must also be processes in place to block assets in the terms established in sanctions programmes and furnish procedures to block the funds of persons, entities or groups subject to these measures.

Group entities must implement internal controls and prevention mechanisms. Controls and specific measures must be implemented for the prevention and detection of deficiencies in systems and negligent or irregular action taken by employees that may result in a failure or malfunctions in the application of international restrictions.

- **Consolidated management of know-your-customer risks:** Consolidated management of know-your-customer risk constitutes a principle for coordinating and sharing information throughout the Group that helps identify, monitor and reduce risks, and comply with applicable legislation and regulations.

Group entities must immediately provide the parent company with appropriate data concerning high-risk customers and activities, and react promptly to information requests by the parent company to assist the Group to manage regulatory and reputational risk relating to money laundering and terrorist financing. This may include data protection laws and cross-border utilisation, depending on the jurisdiction.

Group entities must establish the same above mentioned discipline for local units/subsidiaries or subsidiaries in third-party jurisdictions that are directly controlled by them in relation to AML/CTF.

Group entities must, in all cases, establish safeguard mechanisms so that information concerning customers and their transactions are kept strictly confidential, subject to privacy laws in the country of origin.

## 5) ROLES AND RESPONSIBILITIES

The following is a description of the roles and responsibilities of functions involved in the matters covered by this framework. Such roles and responsibilities must be exercised respecting the three lines of defence and the need to achieve collaboration between the Corporation and Subsidiaries.

Group entities shall have an appropriate organisational and governance structure to identify, prevent and detect money laundering and terrorist financing, report in line with the requirements established in law, and block or freeze funds or economic resources following application of controls of sanctions or international financial countermeasures.

Group entities shall have at least one person appointed as a head the function level, who will take responsibility for application of this framework, its implementation, and enter into dialogue with local supervisors if necessary.

Group entities may appoint an individual responsible for AML/CTF in specific business areas, which operate under the coordination and dependency of the anti-money laundering and terrorist financing function.

- **First line of defence:**

As a general rule and in the context of AML/CFT, the business and support units are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should know and carry out the policies and procedures and be allotted sufficient resources to do this effectively. As part of the first line of defence, policies and procedures should be clearly specified in writing, and communicated to all personnel. They should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the bank in compliance with regulations. There should be internal procedures for detecting and reporting suspicious transactions.

- **Second line of defence:**

Risk and Compliance & Conduct, as the second line of defence, will provide independent challenge and oversight of the risk management activities performed by the first line of defence. This second line of defence should ensure that risks are managed in accordance with the risk appetite defined by senior management and promote a strong risk culture throughout the organization.

As an independent second line of defence, the Compliance & Conduct function is responsible for monitoring and overseeing risks arising from AML/TF and sanction programmes, assessing the impact on risk appetite and the risk profile of the entity and taking account of the provisions of this framework. They will develop and implement the necessary policies and procedures to properly manage and control the prevention of money laundering and terrorist financing and sanction programmes.

The Risk function shall be responsible for integrating and consolidating the risks arising from conduct and reputational risks, assessing the impact on risk appetite and the risk profile of the entity, and taking account of the provisions of this framework. They also add conclusions to specific risk information in

such a way as to present a complete picture of the full range of risks to which the entity or the Group is exposed.

- **Third line of defence:**

As part of the third line of defence, the Internal Audit Function regularly assesses that policies, methods and procedures are adequate and effectively implemented for the management and control of the system for the prevention of money laundering and terrorist financing for compliance with sanction programmes in the Group, providing an independent assessment.

## 6) KEY PROCESSES

Group entities must have effective internal regulation in place enabling them to demonstrate that the AML/CTF activities and related processes are properly executed and in line with all applicable laws and regulations including sanction programmes and international financial countermeasures.

The Corporation will draw up reference documents informing Group entities of the best practices identified at corporate level that may be used to develop their own local internal regulations, making any necessary local adaptations necessary.

The Group may also issue additional documents to act as guidelines for the proper interpretation and consistent application of internal policies within the Group.

Local internal regulations drawn up by Group entities must be validated by the corporate function for the prevention of money laundering and terrorist financing before they are approved by the most senior local management committee in relation to AML/CTF. Internal regulations in this area must also be reviewed on a regular basis to ensure they are complete and up to date, with any modifications or updates necessary.

Specifically, Group entities must have the policies in place that cover the following mandatory areas:

- prevention of money laundering and terrorist financing, and specifically covering certain activities of correspondent banks and private banking.
- supervision and assessment of the risks arising from management and prevention of money laundering and terrorist financing and compliance with international sanction programmes.
- Any other policies and procedures that must be drawn up for the purposes of compliance with any regulations at any time or, on the initiative of the Group or the entities, to enhance management, control and supervision of the issues to which this framework refers.

The Group may also issue its subsidiaries with additional documents, to act as guidelines for the proper interpretation and consistent application of internal policies within the Group.

## 7) GOVERNANCE

The Governance applied in the Group should promote efficient governance structures that ensure adequate participation by all relevant functions. Governance must also be compatible with the functions at a local level, with coordinated management and oversight at the Group level.

The governance bodies for the Group's subsidiaries must be structured taking into account local regulatory and legal requirements, as well as the size and complexity of each subsidiary, whilst ensuring that they are consistent with those of the parent company. Any such governance bodies must promote clear and effective decision-making and clarity of accountability.

Carrying out the AML/CTF function properly in terms of decision-making, supervision and control requires a governance structure, which can provide a response in an efficient and agile manner at both a corporate and subsidiary level.

In its application of this framework, Group entities shall identify the governance bodies or committees responsible for defining, monitoring, controlling and overseeing the AML/CTF regulatory risks.

The Board of Banco Santander, S.A. and its committees, in accordance with the provisions of its bylaws and Board regulations, are the most senior decision-making and monitoring bodies in connection with the management and control of money laundering and terrorist financing and compliance with the sanction programme, except in the case of issues reserved for the general meeting.

The Boards of subsidiaries are also the most senior bodies at their level.

The Boards of each entity and of the Group are responsible for the:

- adoption of Corporate Frameworks
- Supervision of compliance with AML/CTF regulations and legislation, including any actions and measures as a result of inspections by supervisory and control authorities, in addition to internal control and assurance functions.
- Approval of AML/CTF risk appetite as part of the broader risk appetite.

The risk supervision body (Board Risk Committee) is responsible for:

- Assisting and advising the Board in the definition and assessment of the policies stipulated in this Framework.
- Assisting the Board with supervision of the application and analysis of the place in the risk profile.
- Monitoring and assessing any regulatory proposals and new applicable regulations, and the potential consequences for the Group.

The audit body (Board Audit Committee) is responsible for:

- Oversight of the effectiveness of the internal control systems, by reviewing them periodically, in order to identify, manage and release the main risks properly.

In addition to the above, the Group and Group entities shall establish appropriate governance required to ensure the proper management and control of AML, CTF, sanction programmes and associated risks. Group Compliance & Conduct shall validate the appropriateness of such Committees in order to ensure that robust governance is in place.

**8) OWNERSHIP**

This document must be approved by the Board of Banco Santander S.A. The Group Anti-Money laundering and Terrorist Financing Committee is responsible for the interpretation of this Framework.

**9) VALIDITY DATE AND PERIODIC REVIEW**

This framework will be effective on a Group-wide basis from the date of its publication.

Its contents will be reviewed periodically, and any changes or modifications will be made as appropriate.

**APPENDIX: DEFINITION OF TERMS**

**Santander Group or the Group:** group of companies comprising Banco Santander, S.A. as the parent company, and the dependent companies over which it has direct or indirect control. For clarification, it comprises the Banco Santander, S.A. parent company, including the Santander Spain organisational units, which are part of said company, and any other unit/subsidiaries of Banco Santander S.A.

**Corporation:** all the governing bodies, organisational structures and employees entrusted by Banco Santander, S.A. to exercise oversight and control across the entire Group, including those functions typically associated with the relationship between a parent company and its subsidiaries.

**Subsidiary:** a dependent company that forms part of the Santander Group or one directly or indirectly controlled by Banco Santander, S.A.

**Governing Body:** Governance Body or group of bodies of a company that are responsible for the supervision and management of the business at the highest level.

**Senior management:** individuals who exercise executive functions in the entity and who are responsible for the daily management of the entity, and who are accountable to the Governing Body.

**C&C:** Compliance and Conduct

**Compliance function:** the group consisting of the Group C&C function and all subsidiary C&C functions.

**Rules:** legal and regulatory requirements (including internal codes).

**Standards:** guidelines and minimum requirements which may be formulated by the Group, industry bodies or other entities and which Santander has a commitment to.