Banca Popolare di Sondrio

This translation of the original Italian document is provided for convenience only. In case of discrepancy, the Italian version prevails

Level I – General regulation

Policy on the prevention of money laundering and the financing of international terrorism

Document Version:	V4
Approval date:	29/12/2020

Updates to the document

Date	Version	Description
05/2011	1	First draft (document entitled "Corporate Policies for the Management of Money Laundering and Financing of Terrorism Risks")
02/2017	2	First update: Harmonisation of the document structure with that of the other general regulations on risk management issued by the bank; cross-referencing to the self-assessment of risks of money laundering and financing of terrorism prescribed by the Bank of Italy and the monitoring of risk indicators at Group level. Incorporation of the "Regulations on protection and control activities for the management of the risks of money laundering and financing of terrorism" (Renamed "General Regulation on the Risks of Money Laundering and Financing of Terrorism")
10/2019	3	Second update: substantial update (and renaming) of the document to ensure that it complies with the changes introduced by the new European and national provisions on money laundering and financing of international terrorism (EU IV Directive) and to bring it into line with the Group's organisational structure.
12/2020	4	Third update of the document to ensure that it complies with the new changes introduced: - by Legislative Decree no. 125/2019 transposing the 5th EU Directive: partial revision in the Glossary of the definition of PEP, introduction of new specific definitions for entities operating in the virtual currency sector and partial revision related to service providers relating to companies and trusts - paragraph 1.7;procedures for updating the information for due diligence, in relation to customers already acquired (paragraph 4.4); introduction of enhanced due diligence measures for certain sectors deemed at risk such as oil, arms, precious metals, tobacco products, etc. (paragraph 4.4.1); partial revision of the reinforced measures in the case of PEPs acting as bodies of the Public Administration (paragraph 4.4.1); - the Bank of Italy provision "Provisions for the storage and sharing of documents, data and information to combat money laundering and terrorist financing" of 24 March 2020 (paragraph 4.7 and related sub-paragraphs 4.7.1, 4.7.2, 4.7.3, 4.7.4); - by the provision "Provisions for sending aggregate data" issued by FIU on 25 August 2020 (paragraph 1.2); - by Decree-Law no. 76/2020 (so-called "Simplification Decree"), converted with amendments by Law no. 120 of 11 September 2020, which introduced innovations on the subject of the methods for fulfilling the obligations of adequate verification in the case of remote operations (paragraph 4.4.3). In addition, the following changes have been made: - added the effective date of the document (paragraph 1.5); - inserted in the Glossary the definition of "money laundering risk", as indicated in the "Provisions on organization, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing" of the Bank of Italy (paragraph 1.7);

		revised paragraph 2 in order to better detail the controls within the group, with particular reference to the subsidiary Banca Popolare di Sondrio (SUISSE); - added, among the tasks of the anti-money laundering function, that of reporting infringements ex art. 49 of Legislative Decree 231/2007 to the MEF (paragraph 3.6); - better explained the classification of countries in relation to geographical risk (paragraph 4.2); - simplified due diligence measures: expressly added the case of executive/concurrent procedures (paragraph 4.4.2); - addition of SECO (State Secretariat for Economic Affairs, Switzerland) lists for controls on counter-terrorism and international embargoes and on transfers of funds (paragraph 4.6); - revision and rationalization of information flows internally and from/to subsidiaries (Annex 1).

Document approval

Updated by:	**Managing Director**		29/12/2020
		[Mario Alberto Pedranzini]	**Date**
Approved by:	**Board of Directors**		29/12/2020
		[Mario Alberto Pedranzini]	**Date**

CONTENT

1. INTRODUCTION, REGULATORY FRAMEWORK AND PURPOSES

1.1. Introduction

Money laundering and the financing of international terrorism are crimes that constitute a serious threat to the economy with destabilizing effects, especially for the banking and financial system, also because of their possible transnational dimension.

Money laundering, through the reinvestment of illegal proceeds in legal activities and the presence of operators and economic bodies colluding with crime, profoundly alter market mechanisms, undermine the efficiency and correctness of financial activity and weaken the economic system. Terrorist financing activities, on the other hand, involve the allocation for terrorist purposes of funds that may be legal or illegal in origin.

The changing nature of money laundering and financing of terrorism, facilitated by technology in continuous evolution, requires constant upgrading of preventive measures to counter such threats.

The recommendations of the Financial Action Task Force (hereinafter also "FATF"), the main international coordinating body on the subject, foresee that public authorities and the private sector identify and assess the risks of money laundering and financing of terrorism to which they are exposed, in order to take appropriate mitigating action.

Anti-money laundering (AML) and counter terrorist financing (CTF) efforts by the Group take place through the introduction of controls to ensure detailed knowledge of the customer ("know your customer" or KYC), traceability of financial transactions and the detection of suspicious transactions.

The intensity of preventive and counter measures must be modulated on the basis of a risk-based approach, focused on hypotheses worthy of greater in-depth analysis and implemented by making the monitoring more effective and efficient. This approach represents the key point for the prevention activities of the obliged parties and for the controls performed by the Supervisory Authorities.

Banca Popolare di Sondrio (hereinafter also the "Bank" or the "Parent Company") and the companies of the Banking Group are strongly committed to avoiding that the products and services offered may be used for the purposes of money laundering and terrorist financing, promoting internally a culture based on full compliance with the provisions currently in force and effective fulfilment of the obligations of passive collaboration, aimed at ensuring in-depth knowledge of customers, the storage of documents relating to all transactions and active collaboration in identifying and reporting any transactions suspected of money-laundering. For this reason, the Bank and the companies of the Banking Group have adopted this policy at a general level (hereinafter also referred to as the "Document") as an expression of their commitment to combating such criminal action.

The Bank is committed to ensuring that the operating organisation and the control system are complete, adequate, functional and reliable, in order to preserve the Bank and the Banking Group from behaviour, conscious or unconscious, of tolerance or involvement in forms of illegality that can damage its reputation and jeopardize its stability. For these reasons, the Bank and the Banking Group have adopted organisational and behavioural rules and monitoring and control systems

designed to ensure compliance with the regulations currently applied by the administrative and control bodies, staff, collaborators and consultants of the companies in the Banking Group.

1.2. Regulatory framework for the fight against money laundering and the financing of international terrorism

The AML and CTF legislation is contained in a wide variety of sources at international, European and national level.

At international level, a fundamental contribution in the process of legislative harmonisation has been provided by the FATF, the main body that is active in the fight against money laundering, the financing of terrorism and the proliferation of weapons of mass destruction. To perform its function, the FATF prepared a set of international standards (the so-called "40 Recommendations"), to which 9 Special Recommendations regarding the fight against the financing of international terrorism were added in 2001. In February 2012 the subject was completely revised with the adoption of *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, summarised in another "40 Recommendations" and accompanied by "Interpretative Notes" which form an integral part of the new standards. The Recommendations also summarise the counter-terrorism standards introduced in 2001 through the Special Recommendations; specific measures have also been taken to counter the proliferation of weapons of mass destruction in accordance with the Resolutions of the United Nations Security Council.

At European level, the regulations on the subject are contained in Directive (EU) 2015/849 of the European Parliament and Council (hereinafter also "IV Directive") dated 20 May 2015, which repealed Directive 2005/60/EC of the European Parliament and Council and Directive 2006/70/EC of the Commission, followed by Directive (EU) 2018/843 of the European Parliament and Council (so-called "V Directive") dated 30 May 2018, which, in amending the previous one, also included among the recipients providers of foreign exchange services between virtual currencies and currencies that are legal tender and digital wallet service providers for the custody of credentials to access virtual currencies.

In this same context, the following regulations are also worth noting:

– Regulation (EU) 2015/847 of the European Parliament and Council of 20 May 2015 concerning the information that has to accompany any fund transfers;

– Delegated Regulation (EU) 2016/1675 of the Commission of 14 July 2016 and subsequent amendments and additions, which supplements the IV Directive by identifying high-risk third countries with strategic deficiencies;

– Directive (EU) 2017/541 of the European Parliament and Council of 15 March 2017 on the fight against terrorism, which establishes minimum rules concerning the definition of crimes and sanctions within the context of terrorist crimes;

– Delegated Regulation (EU) 2018/1108 of the Commission of 7 May 2018, which integrates the IV Directive with regulatory technical standards on the criteria for the appointment of central contact points for electronic money issuers and payment service providers and rules governing their functions;

– Regulation (EU) 2018/1672 of the European Parliament and Council of 23 October 2018, relating to controls on cash entering or leaving the European Union;

– Directive (EU) 2018/1673 of the European Parliament and Council of 23 October 2018 on the fight against money laundering by means of criminal law, which establishes minimum rules concerning the definition of crimes and sanctions for money laundering;

– Regulation (EU) 2018/1805 of the European Parliament and Council of 14 November 2018 on the recognition and enforcement within the European Union of freezing and confiscation orders issued by another Member State as part of criminal proceedings;

– Delegated Regulation (EU) 2019/758 of the Commission dated 31 January 2019 which supplements Directive (EU) 2015/849 of the European Parliament and Council with regard to regulatory technical standards for minimum action and the type of additional measures that credit and financial institutions must take to mitigate the risk of money laundering and terrorist financing in certain third countries.

The rules concerning the fight against money laundering and terrorist financing are completed at a European level by the periodic reports on supranational risk assessment (Supra National Risk Assessment) published every two years by the Commission, as constituent elements of the overall risk-based approach that characterises the anti-money laundering regulation, and by the "Joint Guidelines of the European Supervisory Authorities" based on the specific attributions provided for in the anti-money laundering regulations.

At a national level, the legislative framework is currently represented by Legislative Decree 231 of 21 November 2007 and subsequent amendments and additions and by Legislative Decree 109 of 22 June 2007 and subsequent amendments and additions.

This regulation, at national level, is completed by the "National Risk Assessment" (NRA) prepared by the Financial Security Committee and by the provisions of the competent Supervisory Authorities aimed at fully implementing the anti-money laundering and counter terrorist financing rules defined at primary level. In particular:

- "Provisions regarding organisation, procedures and internal controls aimed at preventing the use of intermediaries for money laundering and terrorist financing" of the Bank of Italy;
- "Provisions regarding customer due diligence to combat money laundering and terrorist financing" of the Bank of Italy;
- "Provisions for the storage and sharing of documents, data and information to combat money laundering and terrorist financing" of the Bank of Italy;
- "Instructions on objective communications" of the Financial Intelligence Unit;
- "Provisions for sending aggregate data" from the Financial Intelligence Unit;
- "Supervisory provisions on sanctions and administrative sanctioning procedure" of the Bank of Italy.

In addition to these secondary provisions, there are the provisions and communications of the Bank of Italy and the FIU containing models and patterns of anomalous behaviour.

1.3. Regulatory framework for embargoes and international financial sanctions

The Charter of the United Nations gives the UN Security Council the power to decide restrictive measures that are binding on all members, with a view to favouring the maintenance or restoration of peace and international security. The Treaty on European Union and the Treaty on the Functioning of the European Union provide that Member States take a common position in interrupting or restricting economic and financial relations with one or more third countries. These measures, which can be imposed on sovereign states, regimes, individual terrorists, terrorist organisations, producers and proliferators of weapons of mass destruction, are intended to:

– safeguard the common values, fundamental interests, independence and integrity of the European Union in accordance with the principles contained in the United Nations Charter;

– strengthen the security of the European Union;

– preserve peace and strengthen international security;

– promote international cooperation;

– develop and consolidate democracy, respect for the law and human rights and fundamental freedoms.

The reference legislation for embargo management can be divided into the following categories:

– European legislation;

– primary and secondary national legislation.

The main European legislation is contained in the following provisions:

– Council Regulation (EC) 2580/2001 of 27 December 2001, which establishes the obligation to freeze capital and prohibit the provision of financial services towards certain natural persons, legal persons, groups or entities that commit or attempt to commit acts of terrorism and of legal persons, groups or entities controlled by the former;

– Council Regulation (EC) 881/2002 of 27 May 2002, which imposes specific restrictive measures on certain persons and entities (listed in the annex to the Regulation) associated with Osama bin Laden, the Al-Qaeda network and the Taliban;

– Council Regulation (EC) 428/2009 of 5 May 2009, establishing a Community regime for the control of exports, transfer, intermediation and transit of dual-use products (new version of the original Council Regulation (EC) 1334/2000 of 22 June 2000 as amended by the Delegated Regulation (EU) 1382/2014 of the Commission dated 22 October 2014);

– Council Regulation (EU) 753/2011 of 1 August 2011, concerning further restrictive measures against certain persons, groups, companies and entities in view of the situation in Afghanistan and the decisions taken by the Sanctions Committee and the 1267 Committee established as

part of the United Nations Security Council[1].

There are also other sources that are constantly updated, originating from the international and European context, that establish a particular regime banning investments in certain industrial sectors or imports from or exports to certain countries.

The primary Italian legislation is contained in the following provisions:

– Law 185 of 9 July 1990 and subsequent amendments and additions containing new regulations on the control of export, import and transit of armaments;

– Legislative Decree 221 of 15 December 2017 and subsequent amendments and additions which reorganised and simplified the regulation of the authorisation procedures for the export of dual-use products and technologies and of the sanctions regarding commercial embargoes, as well as for any type of exportation of proliferating materials[2].

With regard to secondary legislation, one also has to consider the Bank of Italy Provisions mentioned previously and the Bank of Italy Provision of 27 May 2009 containing operational guidelines for exercising stronger controls over the financing of programmes for the proliferation of weapons of mass destruction.

Also worth noting are the regulations issued by the US Authorities, contained not only in the US Patriot Act[3], but also in the provisions relating to economic and commercial sanctions decided on a case-by-case basis by the US Government, through the Office of Foreign Asset Control (OFAC), as part of foreign policy and national security decisions.

The reference regulatory framework, which is correlated with the AML and CTF regulations, provides for restrictive and sanctioning measures against governments of third countries, as well as non-state entities, natural or legal persons, with regard to:

– arms embargoes;

– other specific or general trade restrictions (ban on imports and exports);

– financial restrictions (freezing of assets and resources, prohibitions on financial transactions, restrictions on export credits or investments);

– sanctions against those who finance terrorist or subversive associations and those who export goods in violation of the rules on dual use.

[1] The Sanctions Committee was set up as part of the United Nations Security Council (or UNSC) pursuant to point 30 of the 1988 (2011) resolution of the UNSC, while the 1267 Committee was also set up under the UNSC pursuant to resolutions 1267 (1999) and 1333 (2000) of the UNSC.

[2] This decree also includes the rules previously contained in Legislative Decree 96 of 9 April 2003, Legislative Decree 11 of 12 January 2007 and Legislative Decree 64 of 14 May 2009, which have all been repealed.

[3] The US Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism - 2001), which was issued following the terrorist attacks of 11 September 2001, extended the requirements of the Bank Secrecy Act (BSA - 1970), requiring financial institutions to prepare due diligence procedures and improve information sharing between financial institutions and the US government.

1.4. Purposes

This document has been drawn up in accordance with articles 15 and 16 of Legislative Decree 231/2007 and with the "Regulations on organisation, procedures and internal controls aimed at preventing the use of intermediaries for money laundering and terrorist financing", the "Provisions on customer due diligence (KYC) to combat money laundering and terrorist financing" and the "Provisions for the storage and sharing of documents, data and information to combat money laundering and terrorist financing", issued by the Bank of Italy and the FIU, and it establishes policy guidelines on the Bank's AML and CTF risk management system in terms of:

– general principles of the risk management model and strategic orientation;

– responsibilities and duties of the corporate bodies and company structures;

– operating methods for managing the risk of money laundering and terrorist financing in the context of adequate data verification and storage as well as sharing of documents, data and information.

1.5. Responsibility for and entry into force of the Document

This document is approved by the Board of Directors of Banca Popolare di Sondrio, after hearing the opinion of the Board of Statutory Auditors, and is addressed to all employees and collaborators of the Bank.

The document is reviewed at least once every two years and, in any case, after any significant changes in the regulations, organisational structure and governance of the Banking Group and in individual Group companies' operations.

Any significant modifications and/or additions to the Document are approved by the Board of Directors of the Bank, after consultation with the Board of Statutory Auditors.

Without prejudice to the duties of the Board of Directors in the approval of any amendments and/or additions to the Document, updating and periodically revising it is the responsibility of the Managing Director in collaboration with the Bank's AML function.

Before approval, the Document is submitted to the Control and Risk Committee for its considerations.

The Policy or amendments thereto shall become effective on the 1st day of the month following the month of approval.

1.6. Recipients of the Document

The Managing Director is responsible for distributing this policy to the companies in the Banking Group for subsequent approval, according to a principle of proportionality, taking into account local regulations and particularities, by the relative Bodies with the strategic supervision function, on the basis of following scope of application:

– to all Italian companies subject to the provisions on AML and CTF;

– to banks belonging to the Banking Group based abroad, in compliance with and compatible with

local regulations currently in force.

The subsidiaries of the Banking Group have to inform the Bank about the outcome of transposing this Document.

The Document also has to be made available and easily accessible to all employees and collaborators, both of the Bank and of the companies belonging to the Banking Group, by publishing it on their corporate intranet.

Implementation of the guidelines and principles contained in this policy at Banking Group level is a prerequisite for encouraging adequate coordination between local AML structures and the Bank's AML function and to ensure effective circulation of information at Group level, in order to counter the risk of money laundering and terrorist financing.

1.7. Glossary

- *"Senior manager":* a director or general manager or other employee delegated by the management body or by the general manager to monitor relations with high risk customers; the senior manager has suitable knowledge of the level of money laundering or terrorist financing to which the recipient is exposed and has been given a suitable level of autonomy to take decisions that can affect this level of risk;
- *"AML":* the acronym of Anti Money Laundering, which is commonly used internationally;
- *"Standardised archives":* archives through which the data and information provided for by the "Provisions for the storage and sharing of documents, data and information for combating money laundering and terrorist financing" of the Bank of Italy are made available; they include the unified computer archives already established at the date of entry into force of Legislative Decree No. 90 of 25 May 2017;
- *"Sector supervisory authority":* Bank of Italy, CONSOB and IVASS, as the national authorities responsible for the supervision and control of banking and financial intermediaries, and the European Banking Authority;
- *"Shell bank":* the Bank or entity that performs functions similar to a Bank that does not have a significant organic and management structure in the country where it was established and authorised to carry on the activity, nor is it part of a financial group subject to effective supervision on a consolidated basis;
- *"Customer":* the person who establishes or has ongoing relationships or performs occasional transactions with the Bank; in the case of ongoing relationships or occasional transactions in the joint name of more than one person, each of the joint holders is considered a customer;
- *"Freezing of funds":* the prohibition, by virtue of EC regulations and national legislation, to move, transfer, change, use or manage funds or to have access to them, in order to modify their volume, amount, placement, ownership, possession, nature, destination or any other change that permits use of the funds, including portfolio management;
- *"Freezing of economic resources":* the prohibition, by virtue of EC regulations and national

legislation, to transfer, dispose of or use economic resources in order to obtain funds, goods or services in any way, including, but not limited to, selling, leasing, renting or constituting real rights of guarantee;

- *"Correspondent current accounts and similar relationships":* accounts kept by banks for the regulation of interbank services, used for the settlement of transactions on behalf of customers of the correspondent institutions;
- *"Payable through accounts":* cross-border correspondent banking accounts between banking and financial intermediaries, used to carry out transactions in their own name and on behalf of customers;
- *"Line controls":* controls carried out by the operating structures (e.g. hierarchical, systematic and sample checks), also through units dedicated exclusively to control tasks that report to the managers of the operating structures, or performed within the scope of the back office, incorporated in IT procedures and aimed at ensuring correct execution of transactions;
- *"Controls on risks and compliance":* these aim to ensure, *inter alia*:
  - proper implementation of the risk management process;
  - compliance with the operating limits assigned to the various functions;
  - compliance of company operations with the standards, including those stemming from self-regulation;
- *"CTF":* the acronym of Counter Terrorism Financing, which is commonly used internationally; alternatively, the acronym CFT for Combating the Financing of Terrorism is also used;
- *"Identification data":* the full name, place and date of birth, official address and place of residence if different from the official address, details of ID document and tax code, if issued, or, in the case of persons other than individuals, the company name, registered office and tax code, if issued;
- *"Anti-money laundering decree":* Legislative Decree 231 of 21 November 2007 and subsequent amendments and additions;
- *"Anti-terrorism decree":* Legislative Decree 109 of 22 June 2007 and subsequent amendments and additions;
- *"Delegate for reporting suspicious transactions":* the person appointed by the Body with the function of strategic supervision of Banca Popolare di Sondrio to evaluate any suspicious transactions and their subsequent transmission to the Financial Intelligence Unit, if considered justified;
- *"Cash":* banknotes and coins, in Euro or in foreign currencies, used legal tender;
- *"Anti-Money Laundering Directive":* Directive (EU) 2015/849 of the European Parliament and Council of 20 May 2015 on the prevention of use of the financial system for the purposes of money laundering or terrorist financing, which amends Regulation (EU) 648/2012 of the European Parliament and Council and repealing Directive 2005/60/EC of the European Parliament and Council and Directive 2006/70/EC of the Commission, as amended by Directive

(EU) 2018/843, of the European Parliament and of the Council of May 30, 2018;

- *"Embargo":* the prohibition of trade and imports/exports with countries subject to sanctions aimed at isolating and putting their government in a difficult internal political and economic situation;
- *"Executor":* the party delegated to operate in the name and on behalf of the customer or to whom, in any case, powers of representation are conferred which enable them to operate in the name and on behalf of the customer;
- *"Financing of terrorism":* for the purposes of Legislative Decree 109/2007 and subsequent amendments and additions, terrorist financing is defined as any activity directed, by any means, to the supply, collection, provision, brokerage, deposit, custody or disbursement of funds and economic resources, in any way achieved, destined to be, directly or indirectly, in whole or in part, used for the purpose of carrying out one or more terrorist acts, as envisaged by criminal law, regardless of whether the funds and economic resources are actually used to carry out such acts.
- *"Funds":* financial assets and instruments of any kind, including the proceeds derived from them, owned, held or controlled, even partially, directly or indirectly, or through a third party individual or legal entity by designated subjects, or by individuals or legal persons that act on behalf of or under the direction of the latter (such as cash, cheques, pecuniary credits, bills, payment orders and other payment instruments, deposits with financial institutions or other parties, balances on accounts, receivables and obligations of any nature, securities negotiable at public and private level, financial instruments as defined in Legislative Decree 58 of 24 February 1998, interest, dividends or other income and increases in value generated by the assets, credit, right of set-off, guarantees of any kind, securities and other financial commitments, letters of credit, bills of lading and other securities representing goods, documents showing participation in funds or financial resources, all other export financing instruments, life insurance policies, etc.);
- *"Business control functions":* the set of functions that by legislative, regulatory, statutory or self-regulation provision have control duties. At Banca Popolare di Sondrio, these functions coincide with the compliance function, the AML function, the risk control unit and the internal audit department;
- *"Banking Group":* the Banca Popolare di Sondrio Banking Group pursuant to art. 60 et seq. of Legislative Decree 385 of 1 September 1993 ("Consolidated Banking Act" or "CBA") and subsequent amendments or additions, made up of the Parent Company and its subsidiaries;
- *"EC banking and financial intermediaries":* the parties referred to in art. 3, paragraphs 1 and 2, of the "anti-money laundering directive" established in a European Community (EU + EFTA) country;
- *"Means of payment":* cash, bank and postal cheques, bank drafts and other similar or comparable cheques, postal orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, pledge policies and any other available instrument that makes it possible to transfer, move or acquire funds, cash or cash equivalents, also by electronic means;

- *"Transaction":* the activity that involves handling, transferring or transmitting means of payment or carrying out negotiated transactions with a financial content; the stipulation of a negotiated transaction with a financial content, which is part of a professional or commercial activity, is also considered a transaction;
- *"Fractionated transaction":* a single economic transaction in terms of value, of an amount equal to or greater than the limits established by the anti-money laundering decree, which is carried out by splitting it into several transactions, each of which is lower than the above limits, made at different times and within a limited time frame of seven days, without prejudice to the existence of a fractionated transaction when there are sufficient elements to consider it as such;
- *"Occasional transaction":* a transaction that is not linked to an ongoing relationship; an intellectual or commercial service in favour of the customer, even with instant execution, would also be considered an occasional transaction;
- *"Suspicious transaction":* a transaction that, because of its characteristics, amount, nature and links with other transactions or fractioning of the same or any other circumstance known due to the functions performed, also taking into account the economic capacity and the activity performed by the subject to which it refers, on the basis of the elements acquired pursuant to the anti-money laundering decree, induces one to believe, suspect or have reasonable grounds to suspect that money laundering or terrorist financing operations are being carried out or attempted or that the funds derive from criminal activity, regardless of their amount;
- *"Related transactions":* transactions that are connected to each other for the pursuit of a single objective of a legal-financial nature;
- *"Corporate bodies":* all of the Bodies with strategic, management and control functions;
- *"Supervisory body":* the Body established pursuant to Legislative Decree 231 of 8 June 2001;
- *"Control body":* the corporate body which has, among other things, responsibility for monitoring the completeness, adequacy, functionality and reliability of the internal control system. At Banca Popolare di Sondrio, the control body is the Board of Statutory Auditors;
- *"Management body":* the corporate body or its members who are responsible for certain management tasks or to whom management tasks are delegated, such as implementation of the guidelines decided in the exercise of the strategic supervisory function. At Banca Popolare di Sondrio this body is represented by the Managing Director and, as regards staff training, by the General Manager;
- *"Strategic supervisory body":* the body performing direction and/or supervision of corporate management (e.g. by examination and resolution regarding the industrial and/or financial plans and/or the strategic operations of the company). At Banca Popolare di Sondrio, the strategic supervisory body is the Board of Directors;
- *"EC countries":* Countries belonging to the European Economic Area (EU + EFTA);
- *"Third countries":* Countries not belonging to the European Economic Area;
- *"High risk third countries":* Countries not belonging to the European Economic Area whose legal systems present strategic shortcomings in the respective national regimes regarding money

laundering and terrorist financing, as identified by the European Commission in the exercise of the powers regulated by articles 9 and 64 of the anti-money laundering directive;

- *"Personnel":* employees and those who, in any case, operate on the basis of relationships that determine their inclusion in the organisation of the obliged party, not necessarily with regular employment;
- *"Politically exposed persons" (or PEPs):* individuals who have occupied or have ceased to occupy important public offices for less than a year, their families and those who have notoriously close ties with such persons, as listed below:
  - individuals who hold or have held important public offices are those who hold or have held the office of:
    - President of the Republic, Prime Minister, Minister, Deputy Minister and Undersecretary, Regional President, Regional Councillor, Mayor of a provincial capital or metropolitan city, Mayor of a municipality with a population of not less than 15,000 inhabitants and similar offices in foreign countries;
    - Member of Parliament, Senator, European Member of Parliament, Regional Councillor and similar offices in foreign countries;
    - member of the central governing bodies of political parties;
    - judge of the Constitutional Court, magistrate of the Court of Cassation or the Court of Auditors, Councillor of State and other members of the Administrative Justice Council for the Sicilian Region and similar offices in foreign countries;
    - member of the governing bodies of central banks and Independent authorities;
    - ambassador, chargé d'affaires or equivalent positions in foreign countries, senior official of the Armed Forces or similar offices in foreign countries;
    - member of the administrative, management or control bodies of companies controlled, directly or indirectly, by the Italian State or by a foreign state or participated, to a predominantly or total extent, by the Regions, by provincial capitals and metropolitan cities and by municipalities with a total population of not less than 15,000 inhabitants;
    - general manager of ASL (health board) and hospital, university hospital and other national health service bodies;
    - director, deputy director and member of the management body or person performing equivalent functions in international organisations;
  - family members of politically exposed persons include: the parents, the spouse or the person connected in a *de facto* civil union or cohabitation or similar institutions to the politically exposed person, the children and their spouses and persons connected to the children in a *de facto* civil union or cohabitation or similar institutions;
  - subjects with whom politically exposed persons have known ties include:
    - natural persons who, in accordance with this decree, jointly hold beneficial ownership

of legal entities, trusts and related legal arrangements with the politically exposed person, or who have close business relations with the politically exposed person;

  - natural persons who only formally hold total control of an entity known to be *de facto* in the interest and for the benefit of a politically exposed person;

- *"Local Italian Politicians" (or LIP)*: persons who, although not PEPs, operate in contexts closely related to local political life and which therefore present a potentially higher risk of money laundering, identified by the Bank in the following roles: provincial president, provincial councillor and municipal councillor, mayor of a municipality with a population of less than 15,000 inhabitants;
- *"Company and trust service providers":* any individual or legal person who provides a third party with one of the following services in a professional capacity:
  - setting up companies or other legal entities;
  - acting as a manager or director of a company, member of an association or a similar function towards other legal entities or arranging for another person to perform this function;
  - providing a registered office with a business, administrative or postal address and other services related to a company, association or any other legal entity;
- performing the function of a trustee in an express trust or a similar legal entity or arranging for another person to perform this function;
- *"Providers of services relating to the use of a virtual currency":* any natural or legal person that provides third parties, on a professional basis, including online, with services, for the use, exchange, storage of a virtual currency and its conversion from and/or into legal tender currencies or into digital representations of value, including those convertible into other virtual currencies as well as issuing, offering, transferring and clearing services and any other service relating to the acquisition, negotiation or intermediation in the exchange of the same currencies;
- *"Digital wallet service providers*": any natural or legal person who provides, on a professional basis, including online, services to third parties to safeguard private cryptographic keys on behalf of their clients, in order to hold, store and transfer virtual currencies;
- *"Relationships similar to payable through accounts":* relationships, however denominated, between the Bank and financial intermediaries on which the customer of the correspondent institution is given the right to execute directly even only part of the transactions pertaining to them;
- *"Ongoing relationship":* a long-lasting relationship, falling within the exercise of the banking activity carried on by obliged parties, which does not end in a single transaction;
- *"Correspondence relationships":* accounts held by banks for the settlement of interbank services (bills of exchange, bank drafts, bank orders, payment orders, fund transfers, documented remittances and other transactions), as well as relationships, however denominated, between banking and financial intermediaries used for the settlement of transactions on behalf of the customers of the correspondent bodies (e.g. deposit of securities, investment services, foreign exchange transactions, document collection services, issue or management of debit or credit

cards);

- *"Money laundering":* for the purposes of Legislative Decree 231/2007 and subsequent amendments and additions, money laundering means:
  - the conversion or transfer of assets, while being aware that they came from a criminal activity or participation in such activity in order to conceal or hide the illicit origin of the assets or to help anyone involved in such activity to avoid the legal consequences of their actions;
  - the concealment or hiding of the real nature, origin, location, disposition, movement, ownership of the assets or the rights to them, while being aware that such assets came from a criminal activity or participation in such activity;
  - the purchase, holding or use of assets, while being aware at the time of their receipt that such assets came from a criminal activity or participation in such activity;
  - participation in one of the above deeds, association to commit such deeds, attempt to perpetrate them, aiding, instigating or advising someone to commit such deeds or facilitating their execution.

  This definition also includes self-laundering, where the person involved in money laundering coincides with the person who committed the crime;
- *"Money Laundering and Terrorist Financing Risk"* means the risk arising from the violation of legal, regulatory and self-regulatory provisions aimed at preventing the use of the financial system for the purposes of money laundering, terrorist financing or financing of programs for the development of weapons of mass destruction, or the risk of involvement in episodes of money laundering, terrorist financing or financing of programs for the development of weapons of mass destruction;
- *"Risk appetite framework":* the framework that defines risk appetite, tolerance thresholds, risk limits, risk governance policies and the reference processes needed to define and implement them, all in line with the maximum acceptable risk, the business model and the strategic plan;
- *"Economic resources":* assets of any kind, tangible or intangible and movable or immovable, including accessories, appurtenances and benefits, which are not funds in themselves, but which may also be used to obtain funds, goods or services, owned, held or controlled, even in part, directly or indirectly, or by an individual or legal person, by designated subjects, or by individual or legal persons acting on behalf of or under the direction of the latter;
- *"Internal control system":* the set of rules, functions, structures, process resources and procedures that aim to ensure the following purposes in compliance with the concepts of sound and prudent management:
  - ensuring the implementation of company strategies and policies;
  - containing risk within the limits indicated in the reference framework that establishes the Bank's risk appetite;
  - safeguarding the value of assets and protection from losses;
  - the effectiveness and efficiency of business processes;

  - the reliability and security of company information and IT procedures;
  - prevention of risk that the Bank might be involved, even unintentionally, in illegal activities (with particular reference to those connected with money laundering, usury and terrorist financing);
  - compliance of transactions with the law and supervisory regulations and with internal policies, regulations and procedures;
- *"Designated persons":* individuals, legal persons, groups and entities designated as recipients of the freezing of funds on the basis of EU regulations, UN resolutions and national legislation;
- *"Operating structures":* the Bank's branches; they represent the first and most important level of control for the prevention and countering of money laundering and terrorist financing, that are effectively in charge of managing customer relationships;
- *"Ultimate beneficial owner":*
  - an individual or individuals on whose behalf the customer establishes an ongoing relationship or carries out a transaction (effective title holder - type 1);
  - in the event that the customer and/or subject on whose behalf the customer establishes an ongoing relationship or carries out a transaction are entities other than an individual, the individual or individuals to whom, ultimately, the direct or indirect ownership of the entity or its control are attributable or who are the beneficiaries (effective title holder - type 2);. In particular, in the case of corporations or other private legal entities, even if based abroad, and trusts expressed, regardless of their place of establishment and the law applicable to them, the effective title holder - type 2 is identified according to the criteria set out in articles 20 and 22, paragraph 5, of Legislative Decree 231/2007; the same criteria apply, insofar as they are compatible, in the case of partnerships and other legal entities, public or private, even if they have no legal status;
- *"Bearer security":* a credit security entitling the holder to exercise the right mentioned therein on the basis of which its mere submission and transfer is carried out by delivery of the security;
- *"FIU":* the Financial Intelligence Unit for Italy, set up at the Bank of Italy;
- *"Virtual currency":* the digital representation of value, not issued or guaranteed by a central bank or a public authority, not necessarily connected to a currency accepted as legal tender, used as a mean of exchange for the purchase of goods and services or for investment purposes and transferred, stored and traded electronically.

2. THE BANKING GROUP'S AML AND CTF RISK MANAGEMENT MODEL

The Banking Group adopts a unified approach to anti-money laundering and counter terrorist financing with guidelines, rules, processes, controls and IT tools that are as consistent as possible across the Group. To this end, the companies belonging to the Banking Group are required to implement this Document, adapting it to their corporate context and, in the case of foreign subsidiaries, to the particularities of local regulations, submitting it to the approval of the Body with strategic supervision functions. The subsidiaries of the Banking Group inform the Bank of the outcome of transposing anti-money laundering and counter-terrorism strategies and policies.

Strategic decisions at Banking Group level regarding AML and CTF risk management and the related controls are left to the corporate bodies of the Parent Company. The corporate bodies of the subsidiaries of the Banking Group have to be aware of the decisions made by the Parent Company's corporate bodies and they are responsible, each according to their own sphere of competence, for the implementation of strategies and policies for managing AML and CTF risk in accordance with their own company situation. In this perspective, the Parent Company, through the Managing Director and the person in charge of its AML function, involves and makes the corporate bodies of Group companies aware of the decisions made regarding policies, processes and procedures for managing AML and CTF risk.

The Parent Company, also through its own AML function, defines and approves at Banking Group level:

- a Group methodology for assessing the risk of money laundering and terrorist financing;
- general standards for adequate verification, storage and sharing of documents, data and information documents, data and information and the identification and reporting of suspicious transactions;
- formalised procedures for coordinating and sharing relevant information on the subject within the Banking Group.

Within the Banking Group, the specific tasks assigned to the AML function are performed on the basis of two separate models, designed to take into account the operational and territorial structure of the Banking Group. In particular:

1) for specifically identified subsidiaries, whose operations are characterised by a high level of integration with the Parent Company, outsourcing of the risk monitoring activities in terms of money laundering and terrorist financing to the Parent Company's AML function is envisaged, at the same time appointing an internal contact person at the subsidiary;

2) for the other subsidiaries for which a regulatory obligation is envisaged and for foreign subsidiaries, it has been decided that autonomous AML functions are set up and a person in charge of each of them is appointed.

In the first case, AML and CTF risk monitoring activities in the subsidiaries are carried out by the Parent Company's AML function with such activities being regulated by specific outsourcing contracts. These provide for the appointment of an anti-money laundering contact person who,

working in close functional coordination with the Parent Company's AML function oversees the processes connected with the AML and CTF regulations within each subsidiary.

In addition to defining the guiding principles and standards of conduct that the subsidiaries must follow when handling the main obligations in this area, the Parent Company's AML function:

– identifies and updates the first and second level control system;

– defines the requirements of the tools supporting customer due diligence and profiling processes and intervenes in the assessment of customers that present a high risk profile;

– supervises the document, data and information storage archive for the fulfilment of anti-money laundering obligations;

– prepares periodic summary reports, or specific reports in the event of particularly serious events, to be sent to the corporate bodies and senior management.

The internal managers appointed at the subsidiaries have the task of verifying the correct performance of the service by the AML function outsourced to the Parent Company and adopt suitable organisational precautions to guarantee that the corporate bodies maintain their powers of guidance and control.

For the subsidiaries of the Banking Group to which the second model applies, on the other hand, the AML function is established and a manager (who may also be delegated to report suspicious transactions) is appointed, with the following duties:

– functionally reporting to the person in charge of the Parent Company's AML function and informing them of the results of the control activities performed and of any significant event;

– ensuring that the head of the Parent Company's AML function has access to all relevant databases;

– liaising with the competent supervisory authorities in coordination with the Parent Company's AML function.

With regard to the reporting of suspicious transactions, the organisational model at Banking Group level envisages the appointment by the Board of Directors of each subsidiary subject to the relative regulatory obligations, after consulting the Board of Statutory Auditors, of a person in the company delegated to report suspicious transactions, so as to ensure suitable coordination mechanisms to safeguard the homogeneity and consistency of the analysis logic used. In order to examine transactions and anomalous relationships in detail from a Banking Group perspective, the person delegated at the Parent Company may interface with the STR delegates at the subsidiaries, in order to share data and information relating to common customers against whom a reporting procedure has been initiated.

In general, for the performance of its duties, the Parent Company's AML function has access to all activities and any information relevant to the performance of its duties.

The Parent Company establishes a shared information database, which allows all companies of the Group to evaluate customers in the same way. With regard to foreign subsidiaries, the Parent Company ensures that their procedures are in line with Group standards and allow information to be

shared within the Group, including that pertaining to reports of suspicious transactions transmitted or those considered groundless, together with the reasons for the decision.

All of this subject to compliance with the limits imposed or the specific obligations provided for by the foreign law applicable in the countries where the subsidiaries are resident.

In any case, the confidentiality of the identity of the subjects participating in the reporting procedure is guaranteed.

If the non-EU jurisdictions do not allow foreign subsidiaries to comply with general standards or to share relevant information with the Parent Company, the latter communicates this to the Bank of Italy and adopts additional measures to reduce the risk of money laundering and terrorist financing, as provided for by the Delegated Regulation (EU) 2019/758 of the Commission dated 31 January 2019.

In particular, with reference to the Swiss subsidiary Banca Popolare di Sondrio (SUISSE) - and its branch located in the Principality of Monaco - in light of the regulatory limits on the sharing of data and information with the Parent Company in force in both legal systems, the Parent Company has adopted a number of additional measures, among those indicated in article 8 of the aforementioned Delegated Regulation, namely:

- neither the Parent Company nor the other companies belonging to the Group rely on the due diligence measures taken by BPS (SUISSE), implementing due diligence measures autonomously and directly with regard to each customer (article 8 letter b);

- periodic on-site visits are planned by the Anti-Money Laundering function, in addition to the periodic audits by the Internal Audit function, aimed at ascertaining that BPS (SUISSE) effectively assesses and manages the risks of money laundering and terrorist financing; training is also shared with the homologous local function, so as to increase and standardize the ability to identify risk indicators in relation to money laundering and terrorist financing (article 8 letter c);

- BPS (SUISSE) is required to determine the origin and destination of the funds to be used within the framework of the business relationship or occasional transaction (Article 8 letter e);

- the Swiss subsidiary has been carrying out a continuous and reinforced control of the business relationship and of the operations until it is reasonably certain that it understands the risk of money laundering and the financing of terrorism which may be related, in compliance with the strict local regulations (article 8 letter f);

- the subsidiary provides the Parent Company with aggregate information on the number of reports transmitted (article 8, letter g), together with the relative motivation and the consequent actions taken;

- the subsidiary has effective systems and controls in place to identify and report suspicious transactions (article 8 letter i);

- BPS (SUISSE) retains, in accordance with the applicable Swiss law, the risk profile and due diligence information of its customers for ten years after the termination of the relationship (article 8 letter j).

Lastly, the head of the Parent Company's internal audit department directs and coordinates the activities of the internal audit functions present in the subsidiaries to ensure uniformity of controls and adequate attention to the various types of risk, including those attributable to failure to comply with legislative provisions on the prevention of money laundering and the financing of international terrorism.

3. ROLES AND RESPONSIBILITIES OF BODIES, FUNCTIONS AND BUSINESS STRUCTURES

3.1. Strategic Supervisory Body (SSB)

The SSB, i.e. the Board of Directors, approves and periodically reviews the strategic guidelines and governance policies of the risks associated with money laundering and terrorist financing.

In this context, the Board of Directors:

- approves a specific anti-money laundering policy that illustrates and motivates the choices that the Bank intends to make with regard to the various key profiles of the organisational structures, procedures and internal control, as well as customer due diligence and data storage in order to assess the consistency with the actual exposure to money laundering risk;
- approves the guidelines of the internal, organic and coordinated control system needed to detect and manage money laundering risk and ensures its effectiveness over time;
- approves the setting-up of the AML function, identifying duties and responsibilities, as well as methods of coordination with the other control functions;
- approves the principles for managing relationships with "high risk" customers, specifying any types of customers with which the Bank should not maintain relationships;
- decides on the appointment and revocation of the person responsible for reporting suspicious transactions and the person responsible for anti-money laundering, having heard the opinion of the control body;
- ensures the allocation of tasks and responsibilities in a clear and appropriate manner, ensuring the separation between the operating structures and the control functions;
- ensures an adequate, complete and timely system of information flows to the corporate bodies and among the various control functions;
- ensures protection of the identity of the person reporting a suspicious transaction;
- examines, at least once a year, the reports of the activity carried out by the person in charge of the AML function and the checks carried out by the competent functions, as well as the document on the assessment of money laundering risks;
- ensures that any anomalies or deficiencies found as a result of second-level controls are immediately are immediately brought to its attention and that corrective measures are taken accordingly, assessing their effectiveness;

- evaluates the risks relating to operations with third countries considered to be at high risk of recycling, identifying the safeguards to mitigate them, and monitors their effectiveness.

3.2. Management Body (MB)

The MB, in the person of the Managing Director:

- handles implementation of the strategic guidelines and policies for the management of money laundering risk as approved by the Board of Directors and is responsible for the adoption of all steps needed to ensure the effectiveness of the organisation and the anti-money laundering control system;
- looks after the definition of a system of internal controls designed for the prompt detection and management of the risk of money laundering and terrorist financing and ensures its effectiveness over time, in line with the evidence drawn from the self-assessment of AML/CTF risks;
- ensures that the operating procedures and information systems allow correct fulfilment of the KYC obligations for customer due diligence and the storage of documents and information;
- as regards the reporting of suspicious transactions, the Managing Director defines and follows the implementation of a procedure that is appropriate for the specific nature of the activity, size and complexity of the Bank to ensure certainty of reference, consistency of behaviour, generalised application to the entire structure, full use of all relevant information and the ability to reconstruct the evaluation process; also adopts measures to ensure compliance with the confidentiality requirements of the reporting procedure, as well as tools, including IT tools, for detecting anomalous transactions;
- defines and takes care of implementation of the initiatives and procedures needed to ensure timely fulfilment of the communication obligations to the Authorities pursuant to the anti-money laundering legislation;
- defines the anti-money laundering policy subject to the approval of the Board of Directors and ensures its implementation;
- defines the information flows that ensure that all of the company structures involved and the control bodies are well aware of the risk factors;
- defines and takes care of implementing the procedures for managing relationships with "high risk" customers, in accordance with the principles established by the strategic supervisory body;
- establishes appropriate tools to allow verification of the activity carried out by personnel in order to detect any anomalies that emerge in their conduct, the quality of communications addressed to the contacts and to the company structures, as well as in personnel relationships with customers;
- ensures, in the case of remote operations, the adoption of specific IT procedures for compliance with anti-money laundering legislation, with particular reference to the automatic identification of anomalous transactions.

The Managing Director acts in collaboration with the Control and Risks Committee and reports to the Board of Directors on the initiatives and interventions necessary to guarantee the completeness, adequacy, functionality and reliability of the internal control and risk governance system.

The MB, in the person of the General Manager, in collaboration with the AML function and the personnel department, establishes staff training programmes on the obligations envisaged in AML regulations on a continuous and systematic basis.

3.3. Control Body (CB)

The CB, i.e. the Board of Statutory Auditors, monitors compliance with the regulations and the completeness, functionality and adequacy of the anti-money laundering control systems. In this context, the Board of Statutory Auditors:

- uses the internal structures to carry out the checks and assessments that are necessary;
- uses information flows from the other Corporate bodies, from the head of the AML function and from other corporate control functions;
- evaluates the suitability of the procedures for customer due diligence, for the storage of document, data and information and for reporting suspicious transactions;
- analyses the reasons for any deficiencies, anomalies and irregularities found and promotes the adoption of appropriate corrective measures.

Its opinion is also required in the decisions to appoint the person responsible for the AML function and the person responsible for reporting suspicious transactions and in the definition of the overall structure of the management system and control of money laundering risk.

Pursuant to art. 46 of the AML Decree, members of the control body communicate without delay to the Bank of Italy any situations that they become aware of in the exercise of their duties that could represent serious, repeated, systematic or multiple violations of the law and the related implementing provisions.

3.4. Supervisory Body (SB)

The SB established under Legislative Decree 231/01 continuously monitors compliance with the processes envisaged by the Organisation, Management and Control Model adopted by the Bank.

In the event that a predicate offence is still committed, it analyses the reasons to identify the most appropriate corrective measures. To carry out these activities, the Supervisory Body receives suitable information flows from the various company structures and/or functions and can access without limitation all the data and information relevant for the performance of its duties.

Lastly, the Supervisory Body forwards to the person in charge of reporting suspicious transactions (known as the "STR manager") any reports of suspicious transactions detected independently in the exercise of its duties.

3.5. Internal Audit Department

With regard to preventing and combating money laundering and terrorist financing, the internal audit function has the task of continuously verifying the adequacy of the company's organisational structure and its compliance with the regulations, as well as overseeing the functionality of the entire internal control system.

The internal audit function periodically checks the adequacy and effectiveness of the AML function.

Through systematic checks and inspections, it verifies:

- constant observance of the obligation of due diligence, both when the relationship is being set up and during its development over time;
- effective acquisition and orderly filing of the documents, data and information required by legislation;
- the degree of effective involvement of the staff and of managers of the central and peripheral structures in the implementation of communication and reporting obligations.

The interventions, both on site and remotely, are subject to planning, in order to allow all the operating structures to be evaluated in a reasonable period of time; moreover, the frequency of the initiatives must be higher for operating structures that are more exposed to the risk of money laundering and terrorist financing, as well as high risk relationships.

It also carries out follow-ups to verify the adoption of the corrective measures envisaged for any anomalies found, and reports at least once a year to the corporate bodies on its activity and results, without prejudice to complying with the confidentiality obligations laid down in the AML decree.

3.6. Anti-money laundering (AML) function

The AML function is part of the second level of the internal control system, it reports directly to the bodies with strategic supervision, management and control functions and has access to all of the Bank's activities, as well as to any information that may be relevant to the performance of its duties.

It is organised in accordance with the principle of proportionality and is, in any case, independent and equipped with resources that are qualitatively and quantitatively adequate for the tasks to be performed, which can also be activated autonomously.

Personnel performing tasks related to the AML function are adequate in terms of number, technical-professional skills and updating, also through continuous training programmes.

The role and tasks of the function are described in the specific "Regulations of the Anti-Money Laundering Function", approved by the Board of Directors.

The AML function continuously verifies that the company's procedures are consistent with the objective of preventing and combating the violation of anti-money laundering and anti-terrorism regulations. In particular:

- it identifies the applicable rules and assesses their impact on internal processes and procedures;
- it collaborates in defining the internal control system and procedures aimed at preventing and combating money laundering risks;

- it continuously verifies the adequacy of the risk management process and the suitability of the internal control system and procedures and proposes organisational and procedural changes aimed at ensuring adequate risk management;
- together with the STR manager, it performs checks on the functionality of the reporting process and on the appropriateness of the assessments made by the first level controls on customers' transactions;
- it collaborates in the definition of the policies for managing the risk of money laundering and the various steps that make up the process of managing this risk;
- together with the other company departments concerned, it performs the annual self-assessment of the money laundering risks to which the recipient is exposed;
- it provides support and assistance to the corporate bodies and senior management;
- it assesses in advance the risk of money laundering relating to the offer of new products and services;
- it verifies the reliability of the information system for the fulfilment of customer due diligence (KYC), document, data and information use and storage, and reporting suspicious transactions;
- it submits the aggregated data concerning the overall operations to the FIU on a monthly basis, pursuant to the “Provisions for submitting aggregate data” published by the FIU on 25 August 2020;
- based on instructions from the FIU, it sends the FIU objective communications concerning transactions at risk of money laundering;
- together with the company departments responsible for training, it takes care of preparing an adequate training plan to update the skills of employees and collaborators on an ongoing basis;
- it promptly informs the corporate bodies of violations or significant deficiencies found in the exercise of its duties;
- it prepares information flows for the corporate bodies and senior management;
- it carries out activities of customer due diligence in relation to particular circumstances, whether objective, environmental or subjective, in which the risk of money laundering is particularly high;
- reports breaches pursuant to article 49 of Legislative Decree 231/2007 to the Ministry of Economy and Finance.

The AML function draws up and submits to the Management Body and to the Strategic Supervisory Body a document that defines in detail the responsibilities, tasks and operating procedures in the management of money laundering risk (the so-called "AML Manual").

In assessing the adequacy of internal procedures for preventing and combating the risk of money laundering, the AML function, together with the internal audit department, can carry out on-the-spot checks to verify their effectiveness and functionality.

At least once a year, the function presents the bodies with strategic supervisory, management and control functions with a report on its initiatives, the anomalies found and the corrective measures to be taken, as well as on staff training. The report also includes the outcome of the self-assessment.

3.7. Head of the AML function

The Head of the AML function is appointed by the Strategic Supervisory Body, having heard the opinion of the Control body, and has to satisfy the requirements of independence, authority and professionalism.

Within twenty days of passing the resolution, the Bank submits to the Bank of Italy the decision to appoint or revoke the Head of the AML function.

He is one of the managers of corporate control functions, so he is placed in an adequate hierarchical and functional position, he has no direct responsibility for the operating structures and is not hierarchically dependent on persons in charge of these areas. He reports directly to the corporate bodies without restrictions or intermediaries.

Staff called upon to work in the AML function, even if normally in operational areas, report directly to the Head of the AML function for all matters relating to these tasks.

3.8. Person responsible for reporting suspicious transactions (STR manager)

Pursuant to article 36 of the anti-money laundering decree, the person responsible for reporting suspicious transactions (or STR manager) is the legal representative of the recipient company or a delegate of the recipient company; the person in charge of the AML function can also be delegated to perform this role. The power is delegated by the Board of Directors, having heard the opinion of the Board of Statutory Auditors.

The STR manager has to satisfy the appropriate requirements of independence, authority and professionalism and carries out his own activity with independent judgement and in compliance with the confidentiality obligations laid down by the anti-money laundering decree, also with respect to management and other company functions. The role of the STR manager is adequately formalised and made known within the structure and to the branch network. The appointment and revocation of the STR manager are promptly communicated to the FIU in the manner indicated by it.

The STR manager has no direct responsibility in operational areas and is not hierarchically dependent on persons belonging to them.

The STR manager:

- evaluates, in the light of all available elements, any suspicious transactions communicated by the person in charge of the branch or of another operating point or organisational unit or structure responsible for handling customer relations (the so-called "first level");
- evaluates, in the light of all available elements, any suspicious transactions that he has otherwise become aware of in the course of his day-to-day work;
- sends the FIU reports on matters that are deemed to be grounded, omitting any indication of the names of the persons involved in the transaction reporting procedure;
- maintains evidence of the assessments made in the context of the procedure, even if no report is sent to the FIU;
- acquires all useful information from the structure that carries out first level analysis of

anomalous operations and from the AML function;

- has free access to information flows to the corporate bodies and to corporate structures and/or functions that may be significant for the prevention and countering of money laundering (for example, requests received from judicial authorities or investigative bodies) and terrorist financing;
- also uses in the evaluations any elements that can be inferred from freely accessible information sources;
- plays an interlocutory role with the FIU and promptly responds to any requests for further information coming from it.

The STR manager communicates, with suitable organisational methods to ensure compliance with the obligations of confidentiality set forth in the anti-money laundering decree, the outcome of his assessment to the first level manager that gave rise to the report.

In compliance with the confidentiality obligations laid down in the anti-money laundering decree on the identity of the parties taking part in the transaction reporting procedure, the STR manager - also through the use of suitable information bases - provides information on the names of the customers subject to reporting suspicious operations to the managers of the competent structures for the attribution or updating of the customers' risk profile.

3.9. Risk Control Unit

With reference to the monitoring of AML and CTF risks, the risk control unit collaborates with the AML function and its manager:

- for the definition of risk assessment methods for money laundering and terrorist financing, fostering synergies with the tools and methods specific to operational risk management;
- to integrate the non-compliance risk assessment and management model into the Risk Appetite Framework;
- in the analysis of the risks associated with new products and services to be launched on the market, also with reference to the entry into new activities and new markets, both upon request and through a structured process of clearing, collaborating in identifying potential risks for the Bank and customers and providing quantitative assessments, where applicable.

3.10. Operating structures

The bank's operating structures represent the first and most important level of corporate governance for the prevention and counteraction of money laundering and financing of terrorism, as operational units that are effectively in charge of managing customer relations. In particular, they:

- implement operational instructions on anti-money laundering and anti-terrorism, imposed by external and internal regulations;
- fulfil the obligations of customer due diligence, both in establishing ongoing relationships and relationships with occasional customers, constantly monitoring the situation throughout the life of

the relationships, also through the use of IT tools specifically designed for this;

- acquire and ensure orderly filing of the documents, data and information required to comply with the obligations of customer due diligence in accordance with the provisions of internal rules, also ensuring that they are kept up-to-date;
- on the basis of the evidence provided by the specifically dedicated tools, carry out periodic evaluations of the risk profile attributed to customers;
- evaluate the transactions carried out by customers, including - but not exclusively - through the IT support tools set up for this purpose, activating, where appropriate, the reporting process for suspicious transactions;
- examine the periodic feedback provided from time to time by the relevant departments or central offices, in order to ensure compliance with the obligations imposed by the legislation on customer due diligence;
- ensure maximum collaboration with the competent Authorities, in the context of investigations, analyses, inspections on money laundering and terrorist financing carried out by them, coordinating with the competent structures and/or functions of the company.

3.11. Branch and area AML contact persons

At each branch of the Bank, a branch contact person is identified by the manager of the operating point, particularly trained in the subject who, coordinating with the central AML function:

- acts as the branch's interlocutor with the AML function, both for requests for advice from the branch and for requests received from the central unit;
- ensures circulation of information within the operating structure, avoiding redundancy in requests for information or assistance, receiving and providing answers to questions within the branch and involving the AML function if its support is needed;
- supports the person in charge of the branch in the continuous evaluation of customer operations and in the detection of any suspicious transactions.

The branch anti-money laundering contact person does not, as such, assume the responsibilities normally assigned to the person in charge of the branch.

The head of the AML function, in agreement with the personnel department, can designate "area" AML contact persons relating to specific territorial areas, usually corresponding to ones used for coordination purposes. Following the indications of the central AML function - to which they belong - they perform on-site assistance and support activities regarding the prevention of money laundering and terrorist financing. The area representatives carry out activities similar to those of the branch contact person, for the benefit of all the branches belonging to the area of competence, supplemented by control and training activities specific to the central AML function.

4. EXPOSURE TO AND MANAGEMENT OF AML/CTF RISKS AND EMBARGO AND

INTERNATIONAL FINANCIAL SANCTIONS

The Bank markets itself as a universal bank, combining its tradition as a cooperative strongly rooted in the territory with a focus on the development of international relations.

Taking into account the nature, size and complexity of the activity performed, as well as the type and range of services provided, the Bank is exposed to a risk of money laundering and terrorist financing monitored by the AML function, also through the self-assessment process, in order to maintain an organisational structure, operating and control procedures as well as information systems capable of guaranteeing compliance with the laws and regulations on the fight against these risks.

For details on the self-assessment process, please refer to the specific paragraph of this Document ("Self-assessment of the risks of money laundering and financing of terrorism"). The AML function - through this periodic process - identifies the current and potential risks to which the Bank is exposed ("inherent risk") and the level of adequacy of its organisational structure ("vulnerability analysis").

The combination of inherent risk assessments and vulnerability of internal controls determines the attribution of the residual risk on the basis of the matrix provided by the Bank of Italy in the "Provisions regarding organisation, procedures and internal controls aimed at preventing the use of financial intermediaries for the purpose of money laundering and terrorist financing".

On the basis of the level of residual risk found, and taking into account the analysis of vulnerabilities, the Bank identifies the corrective or adjustment measures to be taken to prevent and mitigate residual risks. The adjustment measures are implemented by the MB, through the AML function, which is also responsible for monitoring the progress of the adjustment interventions provided for in the plan.

In this context, every six months the AML function updates the results of the last self-assessment process carried out, adjusting the vulnerability analysis in light of implementation of the planned adjustments.

To determine the vulnerability analysis, the Bank assesses the organisational structure, the operational and control procedures as well as the information systems adopted to guarantee compliance with anti-money laundering laws and regulations. In making this assessment, the Bank also takes into consideration the indications and assessments coming from the corporate control functions (e.g. internal audit), as well as taking into account anything that may have been found by the Bank of Italy when carrying out its supervisory controls.

The choices that the Bank has made regarding the various key profiles (organisational structure and operating/control procedures, adequate verification, data storage, suspicious transactions) are provided below to ensure an overall internal control system for prevention of AML and CTF risks able to guarantee compliance with anti-money laundering laws and regulations.

4.1. Organisational procedures and internal control measures

In application of the risk-based approach, the Bank equips itself with an organisational structure, operating and control procedures and information systems capable of ensuring compliance with the

laws and regulations on anti-money laundering and terrorist financing, considering the nature, size and complexity of the activity performed, and the type and range of services provided.

To this end:

– the Bank carries out an overall, periodically updated assessment of its exposure to the risk of money laundering and terrorist financing;

– it gives the AML function the responsibility of ensuring the adequacy, functionality and reliability of anti-money laundering and anti-terrorism measures;

– it formalises the attribution of responsibility for reporting suspicious transactions;

– it attributes to the internal audit department the task of continuously verifying the degree of adequacy of the AML and CTF organisational structure and compliance with the law.

4.2. Assessment of the AML and CTF risk factors and customer profiling

The Bank applies customer due diligence measures proportional to the amount of money laundering and terrorist financing risks found.

In order to grade the depth and extension of the customer due diligence (KYC) obligations, the Bank adopts appropriate procedures aimed at profiling each customer according to the risk of money laundering and terrorist financing, in application of the broader principle of proportionality referred to in the regulations, whose objective is to maximize the effectiveness of company facilities and rationalise the use of resources.

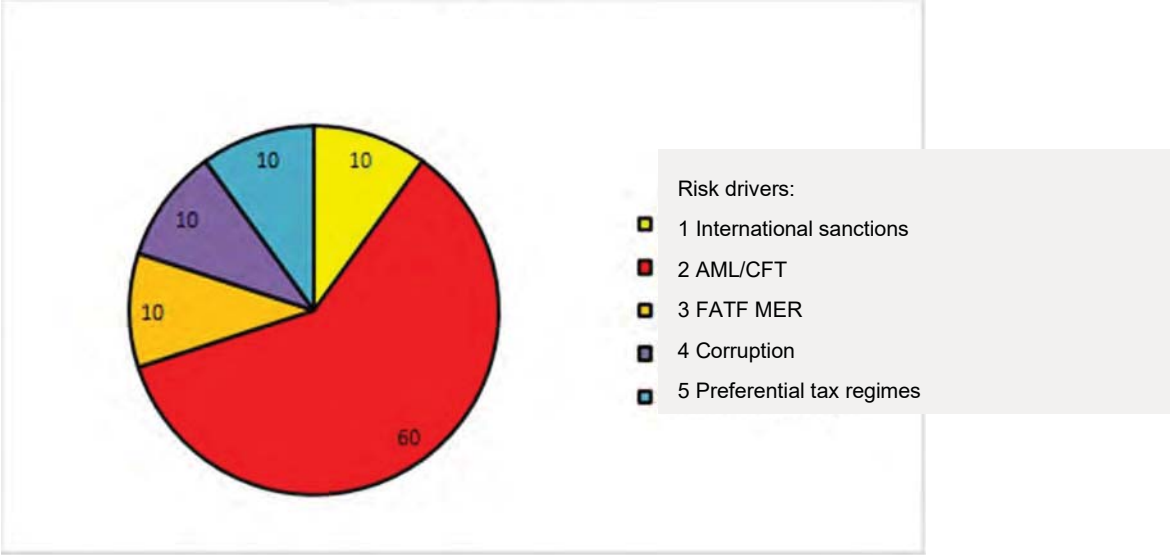
The criteria used to determine the risk attributable to each customer take into consideration a series of factors, including the subjective characteristics of the customer, the executor and the effective title holder, the nature of the relationships established with them, the type of transactions, supplemented by elements that can be deduced from the customer's overall operations (such as their behaviour, the reasonableness of the transaction, the geographical area, the distribution channel, etc.). In the attribution of the profile, in addition to the criteria set out in the anti-money laundering decree and in the "Provisions regarding adequate customer verification", those included in the attachments to this document are considered.

In particular, with regard to the risk factors relating to the country or geographical area, the Bank evaluates:

1) the presence of financial sanctions, embargoes or measures relating to the financing of terrorism or the proliferation of weapons of mass destruction, adopted by the UN, the European Union and the US Treasury Department (so-called "OFAC sanctions");
2) inclusion in lists of countries considered to have a high risk for money laundering and terrorist financing, drawn up by authoritative sources (FATF; list of the European Commission of high-risk third countries);
3) the robustness of the anti-money laundering safeguards in place, as resulting from the mutual evaluation reports adopted by the FATF (so-called MER – Mutual Evaluation Reports and related follow-up reports);

4) the level of corruption and permeability to other criminal activities, as resulting from the assessments of authoritative and independent international organisations, such as Transparency International and the Basel Institute on Governance;
5) the level of fiscal transparency, as shown in the reports approved by the OECD Global Forum on tax transparency and information exchange, and on the evaluation of the commitment to the automatic exchange of information based on the so-called "Common Reporting Standard (CRS)"; to this end, also worth noting is inclusion in the EU list of non-cooperative jurisdictions for tax purposes.

The various factors highlighted above take on the relative weight shown in the following chart:



On the basis of the above factors, the countries are classified into three categories (A, B, C), subject respectively to enhanced, ordinary and simplified due diligence measures. The list of countries, with the relative level of risk assigned, is constantly updated by the anti-money laundering function and circulated within the bank and is also transmitted, for the necessary adjustments, to the subsidiaries

The IT controls available to the Bank make it possible to determine, on the basis of data processing and information acquired during the registry census, the activation of ongoing relationships, the execution of occasional operations and the monitoring of operations, a representative score of the risk level of money laundering or terrorist financing and to classify customers into four classes: Irrelevant, Low, Medium, High.

The information relating to the money laundering and terrorist financing risk profile is made available to the operating structures that are in charge of managing and administering relations with customers in practice. The lowering of a customer's risk level is not permitted except in exceptional circumstances and must be explained in detail to the AML function in writing.

At Group level, each company assumes, for the same customer, the highest risk profile of all those assigned by the various Group companies. Where one of them intends to assign a lower risk profile

than that assigned by other Group companies, the reasons for the decision have to be specifically justified in writing to the AML function.

4.3. Update of profiles and information acquired for customer due diligence

The Bank periodically monitors and updates the scores and rules attributed to the risk profiling system, verifying the adequacy of the risk class assigned on the occurrence of events or circumstances that could change the customer's risk profile.

The timing and frequency of updating the data and information acquired vary according to the risk profile assigned; the update is carried out in any case when it appears that the information previously acquired and used for the KYC verification no longer applies. In particular, it is carried out:

1) at the opening of each new relationship for customers already acquired, regardless of the risk profile;
2) when changes have taken place, as highlighted by the Bank's automatic procedures, relating to:
    a. expiry of ID documents and powers of representation;
    b. changes in beneficial ownership in the case of customers other than individuals;
    c. acquisition of qualities that can change the risk profile, detected by specific internal screening procedures, such as the PEP or LIP qualification.

The following table shows the minimum frequency for updating the data relating to adequate verification, in relation to the risk profiles attributed to customers.

REFERENCE	RISK CLASS	MINIMUM FREQUENCY OF UPDATE
I	Irrelevant	Event by event - when the information is no longer current
L	Low	Event by event - when the information is no longer current
M	Medium	Every 2 years
H	High	Every 12 months

4.4. Customer due diligence procedures

The Bank carries out customer due diligence ("KYC") and of the effective title holder with reference to the relationships and operations inherent in the performance of its institutional activity:

1) on the establishment of an ongoing relationship;
2) upon the execution of an occasional transaction for an amount equal to or greater than € 15,000, regardless of whether it is carried out with a single transaction or with several transactions that appear to be connected to carry out a fractioned transaction or which consists of a transfer of funds, as defined by art. 3, para. 1, no. 9, of Regulation (EU) 2015/847 of the European Parliament and Council, in excess of € 1,000;

3) if the Bank acts as an intermediary or a party in the transfer of cash or bearer securities, in euro or in foreign currency, for a total amount equal to or greater than € 15,000;
4) in all cases where:
    - there is suspicion of money laundering or financing of terrorism, regardless of any exception, exemption or threshold that may be applicable;
    - there are doubts about the completeness, reliability or truthfulness of the information or documentation previously acquired.

To ensure proper performance of the customer verification, the Bank carries out:

a) the identification of customers, potential executors, effective title holders;
b) an assessment of the identity of the customer, the potential executor and the effective title holder on the basis of documents, data or information obtained from a reliable and independent source;
c) the acquisition and evaluation of information on the purpose and nature of the ongoing relationship and, in the event of a high risk of money laundering and terrorist financing, of the occasional transaction;
d) constant monitoring of ongoing relationships, to update the customer's knowledge and the declared purpose of the relationship, to assess any unexpected, abnormal or inconsistent transactions with the customer's previously known economic and financial profile or news of significant events;
e) an update of the data and information collected, with frequency dependent on the risk profile previously associated with the customers.

The Bank asks the client, and the latter is required to provide under their own responsibility, all the necessary and updated information to allow fulfilment of the obligations of adequate verification.

The customer due diligence measures are proportional to the amount of risk of money laundering and terrorist financing, taking into account specific factors with reference to the customer, their conduct, the transaction and the ongoing relationship.

The due diligence obligations are carried out both on new customers before establishing an ongoing relationship or before carrying out an occasional transaction, and those already acquired, when fulfilling the obligations prescribed by Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and by the relevant national transposing legislation. When the bank is unable to comply with the customer due diligence obligations it does not establish an ongoing relationship, i.e. it does not carry out the transaction and, if the ongoing relationship is already in place, it refrains from continuing the relationship. In this case, the bank also considers whether to send a suspicious transaction report, according to the modalities defined by the "Regulations for reporting suspicious transactions".

When the Bank is not able to comply with the customer due diligence obligations, it does not establish the ongoing relationship, i.e. it does not carry out the transaction and, if the ongoing relationship is already in place, refrains from continuing the relationship. In this case, the Bank also evaluates whether to send a suspicious transaction report.

The concrete methods for identifying and verifying the data of the customer, the executor and the effective title holder, for the acquisition and evaluation of information on the purpose and the intended nature of the ongoing relationship and occasional operations and for constant control during the ongoing relationship are governed by the anti-money laundering decree, in the "Provisions regarding adequate customer verification" of the Bank of Italy, in the AML Manual and in the other internal regulations and manuals of the Bank on the subject.

4.4.1. Enhanced customer due diligence measures

The Bank applies enhanced customer due diligence measures in the presence of a high risk of money laundering and terrorist financing, resulting from specific regulatory provisions or independent assessment.

The Bank considers the following high risk factors relating to the customer, the executor, the effective title holder, the products/services, the distribution or geographical channels:

a) ongoing relationships established in unusual circumstances, such as the reticence of the customer or the executor in providing the requested information or the unreasonableness of the transaction;
b) customers and/or effective title holder resident or based in high risk geographical areas;
c) negative reputational indexes relating to the customer, the effective title holder and the executor;
d) structures that can be qualified as capital interposition vehicles;
e) companies that have issued bearer shares or are held by trustees (so-called nominee shareholders);
f) type of economic activity characterised by a high use of cash (gold shops, money changers, companies operating in the gaming/betting sector, both physical and online, agents and/or money transfer companies);
g) type of economic activity attributable to sectors particularly exposed to the risk of corruption;
h) activities of non-profit organisations (NPOs);
i) customer or effective title holder identified as "Local Italian Politicians" (LIP);
j) abnormal or excessively complex ownership structure in relation to the nature of the activity being carried on;
k) services with a high degree of customisation, offered to customers with significant assets;
l) products or operations that could favour anonymity or favour concealment of the identity of the customer or the effective title holder. For example, anonymous prepaid cards issued by foreign intermediaries, bearer shares, transactions referable to services connected with the conversion of legal currency into virtual currency and vice versa;
m) frequent and unjustified cash transactions, characterised by the use of high value euro banknotes, or the presence of damaged or counterfeit tickets;
n) cash payments or values coming from abroad for a total amount equal to or greater than the equivalent value of Euro 10,000. In such cases, the Bank asks the customer for a copy of the

cash transfer declaration provided for by article 3 of Legislative Decree 195 of 19 November 2008 and examines any customer refusal or reluctance to provide documentation;

o) payments received from third parties without a clear connection with the customer or his business;

p) new generation products and business practices, which include the use of distribution mechanisms or innovative technologies for new or existing products;

q) the circumstance of having ceased for over a year one of the public offices provided for by article 1, paragraph 2, letter dd), point 1 of the anti-money laundering decree;

r) transactions involving oil, weapons, precious metals, tobacco products, cultural artifacts and other movable property of archaeological, historical, cultural and religious importance or rare scientific value, as well as ivory and protected species.

The Bank always applies enhanced customer due diligence measures in the cases prescribed, i.e.:

1) occasional relationships and operations involving high-risk third countries, as identified by the European Commission;

2) cross-border relationships with a corresponding bank or financial intermediary based in a third country involving the execution of payments;

3) ongoing relationships or occasional operations with customers and related effective title holders who are politically exposed (PEPs), except in cases where the same are acting as bodies of public administrations. In these cases, the bank adopts adequate verification measures commensurate with the risk actually detected, also taking into account the provisions of article 23, paragraph 2, letter a), no. 2 of the anti-money laundering decree;

4) customers who carry out transactions characterised by unusually high amounts or with respect to which there are doubts about the purpose for which they are, in practice, being performed.

In addition, in the presence of one or more of the high risk factors listed above - and if the transactions differ from the one normally expected, or can be traced back to anomalous behaviour patterns - the Bank applies enhanced customer due diligence measures on relationships regarding:

5) trusts;

6) fiduciary companies not registered in the register pursuant to article 106 of the Consolidated Banking Act;

7) agents and/or money transfer companies;

8) companies operating in the gaming/betting sector, both physical and online;

9) non-profit organisations (NPOs);

10) customers who have already been the subject of a suspicious transaction report in the previous three years and related parties;

11) persons to whom the Bank has received notice of investigations or proceedings by the judicial authority or investigative bodies for money laundering crimes in the three previous years and related parties;

12) persons connected to PEPs;

13) customers resident or based in third countries assessed as high-risk customers by the Bank, according to the criteria illustrated in paragraph 4.2, or transactions involving the countries themselves;
14) customers who, for objective reasons or for further evaluations carried out by the relevant subsidiary or by another Group company, should be subjected to reinforced measures.

The enhanced due diligence measures are reflected in the acquisition of more information about the customer and the potential effective title holder and in a more accurate assessment of the nature and purpose of the relationship; in a higher quality of information requested; in the intensification of the frequency and depth of the analyses carried out in the context of constant control of the relationship and operations. In particular, these measures consist of:

i) the acquisition of a greater amount of information concerning the customer's ownership and control structure. In particular, the documentation used to identify the effective title holder must include a date not earlier than the last two years;
ii) the acquisition of a greater quantity of information relating to the ongoing relationship, to fully understand its nature and purpose, in particular on:
    - the reasons why the customer asks for a certain product or service, especially if their financial needs could be better met in another way or in another country;
    - the origin and destination of the funds;
    - the nature of the activity performed by the customer and the effective title holder;
iii) a better quality of information to be acquired, such as:
    - verification of the origin of the assets and of the customer's funds, used in the ongoing relationship;
    - in the case of frequent and unjustified cash transactions, especially if carried out with high value banknotes, the Bank carries out in-depth investigations with the customer about the reasons behind such transactions;
iv) a greater frequency - at least once a year - of checks on ongoing relationships, in order to promptly detect any suspicion of money laundering and terrorist financing;
v) the need to obtain the authorisation of a senior manager for the opening or continuation of ongoing relationships or for the execution of occasional transactions with customers and related effective title holders who are PEPs;
vi) the need to obtain the authorisation of the AML function for the opening or continuation of ongoing relationships with trusts and intermediaries in the money transfer business;
vii) in the case of cross-border correspondence with banking or financial intermediaries in a third country, the Bank applies appropriate reinforced verification measures provided for in Section IV, Fourth Part of the Provisions on the subject of adequate verification of the Bank of Italy.

4.4.2. Simplified obligations of due diligence

The Bank can apply simplified customer due diligence measures in terms of the extent and frequency of the obligations envisaged, in the presence of a low risk of money laundering and terrorist financing.

The Bank considers the following as low-risk factors and, therefore, applies simplified measures of adequate verification to the following categories of customers or products/services:

1) companies admitted to listing on a regulated market and subject to communication obligations that impose an obligation to ensure adequate transparency of beneficial ownership, or those listed on regulated markets of EU countries and third countries recognised by Consob pursuant to article 70 of the CFA;
2) public administrations, or institutions or bodies that perform public functions, in accordance with European Union law;
3) accounts in the name of executive and insolvency procedures;
4) customers resident or based in EU countries and in third countries equipped with effective systems to prevent money laundering and terrorist financing, characterised by a low level of corruption or permeability to other forms of crime, by an adequate level of fiscal transparency and commitment to the automatic exchange of information on tax matters, based on authoritative and independent sources;
5) banking and financial intermediaries indicated in article 3, paragraph 2, of the anti-money laundering decree - with the exception of those referred to in letters i), o), s) and v);
6) EU banking and financial intermediaries;
7) banking and financial intermediaries based in a third country with an effective regime against money laundering and terrorist financing, except in cases of cross-border correspondence;
8) financial products or services appropriately defined and limited to specific types of customers, aimed at encouraging financial inclusion; this definition includes the "basic current account" and salary or pension backed loans and the delegation of payment.

The simplified customer due diligence measures consist of:

i) the possibility of verifying the data relating to the effective title holder by acquiring a confirmation statement signed by the customer under their own responsibility;
ii) the absence of pre-established deadlines for updating the data collected for adequate verification, except in the case of the opening of new relationships or when the information is no longer current.

In any case, the Bank verifies that the conditions for applying the simplified procedure still exist.

Simplified customer due diligence measures cannot be applied when:

- there are doubts, uncertainties or inconsistencies in relation to the identification data and information acquired when identifying the customer, the executor or the effective title holder;
- the conditions for applying simplified measures are no longer valid, based on the risk indices established by the anti-money laundering decree and the provisions issued by the supervisory authorities;

- the monitoring activities on the overall operations of the customer and the information acquired during the relationship tend to exclude the presence of a low risk case;
- there is suspicion of money laundering or terrorist financing.

4.4.3. Due diligence when transactions are carried out on a remote basis

The Bank pays particular attention in the case of remote operations, i.e. when transactions are carried out by the customer without their physical presence at the Bank (e.g. by mobile phone or online).

The identification obligation is considered fulfilled, even without the physical presence of the client, in the following cases:

1) for customers whose identification data result from public deeds, authenticated private agreements or qualified certificates used for the generation of a digital signature associated with IT documents, pursuant to Article 24 of Legislative Decree No. 82 of March 7th, 2005;

2) for customers in possession of a digital identity, with at least a significant level of guarantee, under the System referred to in Article 64 of Legislative Decree No. 82 of 2005, as amended, and the relevant implementing regulatory legislation, as well as a digital identity with at least a significant level of guarantee or a certificate for the generation of digital signatures, issued under an electronic identification scheme included in the list published by the European Commission pursuant to Article 9 of EU Regulation No. 910/2014, or a certificate for the generation of digital signatures or, finally, identified by means of secure and regulated electronic identification procedures or authorized or recognized by the Agency for Digital Italy[4];

3) for clients whose identification data result from a declaration by the Italian representation and consular authority, as indicated in article 6 of Legislative Decree 153 of 26 May 1997

4) for clients who have already been identified in relation to another relationship, provided that the existing information is up-to-date and adequate in relation to the client's risk profile;

5) for customers who, after electronic identification based on credentials that ensure the requirements set out in Article 4 of Delegated Regulation (EU) 2018/389 of the Commission of 27 November 2017, arrange a transfer to a payment account in the name of the person required to be identified. This method of identifying and verifying identity may be used only with reference to relationships relating to payment cards and similar devices, as well as to payment instruments based on telecommunications, digital or computer devices, with the exclusion of cases in which such cards, devices or instruments can be used to generate the information necessary to directly make a credit transfer or direct debit to and from a payment account;

6) for customers whose identification data are acquired through the methods identified by the Bank of Italy in the "Provisions on adequate verification".

In practical terms, in cases of remote operations, the Bank:

[4] To this end, the bank can identify the customer remotely through an Identity Provider, which operates according to procedures authorized and recognized by the Agency for Digital Italy.

1) acquires the identification data of the customer and the executor and verifies them against a copy, obtained by fax, mail or in electronic format, of a valid ID document;
2) makes additional checks on the data acquired, in one of the following ways:
   - transfer made by the customer through another intermediary based in Italy or in a European country;
   - request for verification and confirmation of data at another intermediary based in a SEPA country ("Single Euro Payments Area"), via "SEDA" electronic messaging ("SEPA Electronic Database Alignment");
   - request to send signed documentation;
   - remote identification in accordance with the audio-video registration procedure governed by Annex 3 of the Provisions regarding adequate customer verification of the Bank of Italy.

4.4.4. Execution by third parties of customer due dilingence obligations

The Bank may resort to third parties for the fulfilment of adequate customer verification obligations, without prejudice to full responsibility for compliance with these obligations, according to the methods and within the limits established by the anti-money laundering decree and the provisions of the Supervisory Authorities.

In no case may the Bank avail itself of third parties located in high-risk third countries.

4.4.5. Constant monitoring during an ongoing relationship

The Bank carries out constant monitoring during an ongoing relationship to keep the customer's profile updated and identify elements of inconsistency that may constitute significant anomalies for the purpose of adopting reinforced adequate verification measures, reporting suspicious transactions and abstention from the execution of the transaction or continuation of the relationship.

Constant control is exercised by examining the customer's overall operations, taking into consideration both ongoing relationships and any specific transactions that may be arranged, as well as acquiring information during the verification or updating of the news for the identification of the customer, the effective title holder and the assessment and check of the nature and purpose of the relationship or transaction.

To this end, the Bank adopts ex-ante and ex-post control procedures, in order to identify, block and highlight suspected money laundering and terrorist financing operations and in relation to limitations on the use of cash and bearer securities.

4.5. Obligations of abstention

If the Bank is in the objective impossibility of carrying out adequate customer verification, it refrains from establishing the relationship or carrying out the transactions and, for the relationships already

in place, takes steps to eliminate them. It also assesses whether to report a suspicious transaction to the FIU.

In any case, the Bank refrains from establishing relationships or carrying out transactions and terminates an ongoing relationship in the following cases:

1) correspondence accounts directly or indirectly attributable to banks of convenience (or "shell banks");

2) legal entities including, directly or indirectly, trust companies, trusts, anonymous companies (or controlled through bearer shares) with headquarters in high-risk third countries as identified by the European Commission in the exercise of the powers regulated by articles 9 and 64 of the anti-money laundering directive.

The Bank also:

3) does not open anonymous accounts or accounts with fictitious or numerical names;

4) does not offer "payable through accounts";

5) does not maintain relationships and does not carry out occasional transactions towards companies that carry out activities such as service providers related to the use of virtual currencies (or "cryptocurrencies");

6) refrains from offering products and/or services or from performing transactions that could favour anonymity;

7) refrains from establishing ongoing relationships or performing occasional remote transactions not supported by adequate recognition mechanisms and procedures.

4.6. Controls on anti-terrorism and international embargoes and fund transfers

In view of the increasing importance of the fight against international terrorism, programmes for the development of weapons of mass destruction and the trading of dual-use products and technologies, the Bank adopts internal control procedures able to identify customers or transactions that have a high risk of involvement in commercial or financial activities that are made by customers in violation of restrictive measures adopted by the international community towards certain countries, individuals and legal persons, entities and organisations.

Such checks, which are complementary to those carried out in the ordinary course of due diligence procedures, can be broken down into:

1) checks on the names: these apply to the names of counterparties involved in the movement of funds, in order to ensure that customers do not operate with those subject to sanctions by international bodies, which involve the obligation to freeze funds and economic resources, or the application of restrictive measures of a different nature (so-called "designated persons"). In this context, the lists of persons and entities subject to restrictive measures applied by the European Union, the UN, OFAC and SECO (State Secretariat for Economic Affairs, Switzerland) are taken into account;
2) checks on the country: these apply to the countries of origin and/or conduct of the affairs of customers, as well as to the countries of origin and destination of the funds they are dealing

with, for the purpose of verifying that they belong to the list of "countries or territories at risk" as they are: (a) characterised by anti-money laundering rules that do not comply with EC standards and/or preferential tax regimes; (b) indicated by international bodies (e.g. FATF, OECD, OFAC, European Union) as being exposed to the risk of money laundering and financing of terrorism and/or not cooperating in exchanges of information, also in tax matters; (c) recipients of international embargoes for low levels of counteraction of terrorist activity or violation of fundamental human rights;

3) transactional controls: these apply to the transfer of funds carried out by customers and to any goods or services underlying them, in order to verify that embargo measures or similar commercial restrictions are not being violated (e.g. prohibitions or restrictions on the import/export of commodities, raw materials and technology) as well as financial (e.g. bans or restrictions on financial services, investments, capital transactions).

As a result of the checks carried out, where significant risk situations are identified, enhanced measures are taken to acquire additional data and information, also through the production of appropriate documentation, and to monitor with particular intensity the trend in relationships with the customer in question, without prejudice to the obligation to report suspicious transactions when certain conditions are met.

In the specific circumstances indicated in the national and EC embargo rules, the freezing of funds and economic resources of the persons or entities affected by restrictive measures is also fulfilled with a ban on making available capital or economic resources to them. Lastly, the procedures for notification, communication or authorisation request to the Authorities in the event that sanctions are applied.

Lastly, in compliance with the provisions of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 concerning the information data accompanying the transfers of funds, the Bank adopts procedures capable of identifying information on the originator and the beneficiary to be included in fund transfers.

4.7. Storage and sharing of document, data and information

The Bank keeps the documents, data and information useful for preventing, identifying or verifying any money laundering or terrorist financing activities and to allow the analyses carried out by the competent Authorities through IT storage systems that ensure:

- complete and timely access to document, data and information by the Authorities;
- timely acquisition of documents, data and information, with an indication of the related date;
- integrity of the documents, data and information and its non-alterability after it has been acquired;
- the adoption of appropriate measures aimed at preventing any loss of documents, data and information;
- transparency, completeness, clarity of documents, data and information and maintaining their historical path.

To this end, the Bank ensures the storage of documents, data and information acquired for ten years from the termination of the ongoing relationship or from the execution of the occasional transaction.

4.7.1. Type of documents, data and information to be retained

In accordance with Article 31(2) of the Money Laundering Decree, the bank retains copies of the documents acquired during the due diligence of the customer, the executor and the beneficial owner.

The bank also stores information on:

1) with respect to ongoing relationships: the operating point at which the relationship was established, the date of establishment and the termination date;
2) with reference to occasional transactions to be subject to adequate verification and to transactions based on ongoing relationships: the date of execution, the amount, the currency, the reason for the transaction and the means of payment used;
3) with regard to occasional transactions for which due diligence is not required, the bank shall keep, in addition to the provisions of point 2) above, the data and information capable of unambiguously identifying the customer and the agent and, where known, the sector of economic activity and the data and information capable of unambiguously identifying the beneficial owner.

The acquisition of the documents, data and information must be completed no later than 30 days after the establishment of the continuing relationship, the execution of the transaction, the variation and the closure of the ongoing relationship.

Storage requirements relate to ongoing relationships and transactions that are part of the bank's institutional activity.

4.7.2. Data and information to be made available to the Authorities

The bank makes available to the Bank of Italy and to the FIU, according to the standards set out in the "Provisions for the storage and sharing of documents, data and information for combating money laundering and terrorist financing" of the Bank of Italy of 24 March 2020, the data and information indicated in Article 5 of these provisions.

4.7.3. Methods for the storage and sharing of documents, data and information

In order to store documents, data and information, the bank uses computerised storage systems, consisting of its accounting and management systems.

In order to ensure that customer transactions can be reconstructed and to facilitate the Bank of Italy's and the FIU's monitoring activities, including inspections, the bank ensures that data and information

are made available to the authorities through a specific standardised archive[5], in accordance with Annex 2 of the Bank of Italy's "Provisions for the storage and sharing of documents, data and information to combat money laundering and terrorist financing" of 24 March 2020.

4.7.4. Exemptions

The bank does not apply the provisions regarding data and information to be made available to the Authorities, in relation to ongoing relationships or transactions entered into with[6]:

1) the following banking and financial intermediaries referred to in article 3, paragraph 2 of the anti-money laundering decree, having their registered office in Italy or in another member state;
   - banks;
   - Poste italiane S.p.a;
   - electronic money institutions as defined by article 1, paragraph 2, letter h-bis), TUB (IMEL);
   - payment institutions as defined by article 1, paragraph 2, letter h-sexies), TUB (so-called IP);
   - securities brokerage firms, as defined by Article 1, paragraph 1, letter e), TUB (SIM);
   - asset management companies, as defined by Article 1, paragraph 1, letter o), Consolidated Law on Finance (SGR);
   - investment companies with variable capital, as defined by art. 1, paragraph 1, letter i) of the Consolidated Law on Finance (SICAVs);
   - investment companies with fixed capital, securities and real estate, as defined by art. 1, paragraph 1, letter i-bis) of the Consolidated Law on Finance (SICAF);
   - intermediaries registered in the register provided for in article 106 TUB;
   - Cassa depositi e prestiti S.p.a.;
   - insurance companies that operate in the classes referred to in Article 2, paragraph 1, of the CAP;
   - micro-credit providers, pursuant to Article 111 of the Consolidated Law on Banking;
   - credit consortia and other entities referred to in article 112 of the Consolidated Banking Act;
   - established branches of banking and financial intermediaries (as per the previous point), with registered office and central administration in another member state or in a third country;
   - banking and financial intermediaries (as per the previous point) with registered office and central administration in another member state, established without a branch in the

[5] So called "ex AUI" (former *Archivio Unico Informatico*- Unified Computer Archive), updated according to the new instructions mentioned above.

[6] Entities identified on the basis of the following S.A.E. codes (i.e. the Economic Activity Subgroup, as indicated in Bank of Italy Circular no. 140 of 11 February 1991): 100, 101, 245, 248, 258, 259, 266, 270, 275, 300, 264, 727, 728.

territory of the Italian Republic;

2) the subjects referred to in article 3, paragraph 8, of the anti-money laundering decree[7];

3) the Provincial Treasury of the State and the Bank of Italy.

4.8. Reporting suspicious transactions

Before carrying out the transaction, the Bank sends to the FIU a suspicious transaction report when it is aware, suspects or has reasonable grounds to suspect the existence of or attempt at money laundering or terrorist financing operations or that the funds being transferred derive from a criminal activity. The suspicion is inferred from characteristics, amount, nature of the operations, also taking into account the economic capacity and the activity carried out by the subject to which it refers.

Frequent and unjustified recourse to cash transactions and the withdrawal or payment in cash of amounts inconsistent with the customer's risk profile constitute elements of suspicion.

The management of the process that can lead to the reporting of a suspicious transaction is attributed to the person delegated to report suspicious transactions who:

– evaluates, in the light of all the available elements, any suspicious transactions that have been detected;

– submits to the FIU the reports deemed to be grounded;

– maintains evidence of the assessments made in the context of the procedure, even if no report is sent to the FIU;

The Bank guarantees all appropriate measures to ensure the confidentiality of the identity of the persons who report a suspicious transaction. In particular, the name of the person reporting can only be revealed when the judicial authority, in this regard, arranging it with a justified decree, deems it indispensable for the purpose of ascertaining the offences for which it proceeds.

It is also forbidden for the persons obliged to report a suspicious transaction and to anyone who is aware of it, to notify the customer concerned or a third party of the report, of sending further information requested by the FIU or of the existence and/or the possibility of investigations into the matter.

The reporting of suspicious transactions and the communication of any additional information requested by the FIU, carried out in good faith by employees or directors, do not constitute a violation of any restrictions on the communication of information imposed by contract or by law, regulatory or administrative provisions; moreover, they do not entail any type of liability, even in cases where the reporting party is not aware of the underlying criminal activity and regardless of whether the illegal activity was actually carried out.

[7] Centralized financial instruments management companies, companies managing regulated markets for financial instruments, entities managing facilities for the trading of financial instruments and interbank funds, companies managing settlement services for transactions in financial instruments, management company of the clearing and guarantee systems for financial instruments.

4.9. Staff training

Effective application of anti-money laundering and counter-terrorism regulations presupposes adequate knowledge of the obligations and responsibilities that may arise from failure to comply with the relevant regulations. Hence the need for suitable training and continuous education measures for all staff, with programs that take into account the evolution of national and international legislation and internal self-regulation (regulations, manuals, procedures, circulars, etc.).

To this end, the Bank organises staff training and training programmes and guarantees the spread of a corporate culture based on compliance with the regulations.

In collaboration with the anti-money laundering and staff service department, the General Manager establishes staff training and education programmes on the obligations provided by the anti-money laundering discipline on a continuous and systematic basis.

In particular, these training programmes:

– ensure greater preparation for employees and collaborators who are in direct contact with customers and for staff belonging to the AML function, who are required to be constantly updated on the evolution of money laundering risks and on the typical patterns of criminal financial transactions;

– ensure a continuous update of personnel regarding the evolution of the legislation and the risks of money laundering and terrorist financing;

– are carried out periodically and systematically and are submitted annually for approval by the management body.

4.10. Information flows

With specific reference to information flows to the FIU, the Bank submits:

– aggregate data concerning its operations, in order to allow the performance of analyses aimed at bringing out possible cases of money laundering or terrorist financing within certain territorial areas, according to the methods and timing defined by the Authority in the "Provisions for sending aggregate data" of 25 August 2020;

– within thirty days from the date of entry into force of the European regulations or the decrees issued by the Ministry of the Economy and Finance, concerning the freezing of funds and economic resources held by individuals or legal persons, groups or entities that carry out activities aimed at terrorist acts or the financing of weapons of mass destruction or the threat of international peace and security, the measures applied, indicating the subjects involved, the amount and nature of the funds or economic resources;

– on a timely basis, the operations, reports and any other available information attributable to the designated subjects or those being designated in the EU regulations or in the decrees issued by the Ministry of the Economy and Finance.

With reference to the information flows within the Bank and the Banking Group, the Bank defined the flows that the corporate structures must exchange to ensure the necessary alignment with regard

to the protection of money laundering and terrorist financing risks, as detailed in Annex 1 ("Information flows").

The AML function has access to all of the Bank's activities and to any information that is relevant for the performance of its duties, also through direct interviews with members of staff. To this end:

- the other structures and/or functions of the Bank must communicate to it, in a timely and complete manner, any material event for the purpose of monitoring the risks in question;
- it may request and receive from the other structures and/or functions any additional information relevant to the performance of its duties.

4.11. Reporting obligations of the Board of Statutory Auditors and reporting systems for violations

The Board of Statutory Auditors supervises compliance with the legislation on money laundering and terrorist financing. In this regard, it communicates without delay to the Bank of Italy all of the facts that it becomes aware of in the exercise of its functions that may integrate serious or repeated or systematic or multiple violations of the provisions provided for by law and the implementing provisions.

If in the performance of its functions it becomes aware of potentially suspicious transactions, it informs the STR manager and the AML function.

The Bank also has specific procedures for reporting internally, by employees and collaborators, potential or actual violations of the provisions laid down to prevent money laundering and terrorist financing (i.e. "whistleblowing").

5. SELF-ASSESSMENT OF THE RISKS OF MONEY LAUNDERING AND FINANCING OF TERRORISM

In accordance with the criteria and methods established in the Regulations on Organisation, Procedures and Controls issued by the Bank of Italy, the Bank carries out a self-assessment of the risk of money laundering and financing of terrorism to which it is exposed.

As regards the Banking Group, the Parent Company coordinates the process carried out by each of the companies in the Group and performs a Group self-assessment, the results of which are assessed by the Board of Directors, after examination by the Control and Risks Committee, and by the Board of Statutory Auditors.

The self-assessment is carried out on the basis of a methodology that includes the following macro-activities and aspects:

a) identification of inherent risk (on a scale of 4): the current and potential risks to which the Bank is exposed are identified, also taking into consideration the elements provided by

external information sources. In particular, at this stage, factors such as the type of customer, products and services offered, the Bank's operations, distribution channels and geographical area are taken into consideration;

b) vulnerability analysis (on a scale of 4): in this phase, the adequacy of the organisational structure and of the prevention and monitoring measures with respect to the risks identified previously are analysed in order to identify any vulnerabilities; the attribution of the level of vulnerability is accompanied by an overall judgement on the effectiveness of the control structures in place, as well as a brief illustration of any weaknesses identified, with an explanation of the reasons that led to the score;

c) determination of residual risk (on a scale of 4): depending on the line of business, the Bank evaluates the level of residual risk to which it is exposed due to the inherent risk level and the strength of mitigation measures, making use of the residual risk determination matrix prepared by the Bank of Italy;

d) remedial action: once the residual risk has been determined, the Bank defines appropriate corrective actions and remedies to be adopted in the event of any existing critical issues, as well as appropriate measures to be taken to prevent and mitigate the risk of money laundering.

Given that the Bank does not have a structure organised by business sector (such as retail banking, corporate or investment banking), the identification and assessment of inherent risk are performed in relation to the Bank's main lines of business: in particular, certain lines of business are associated with specific types of products or services that are considered more significant on the basis of certain characteristics (volume, core activity of the Bank, etc.).

The self-assessment process is updated annually by the AML function and sent to the Bank of Italy by 30 April of the year after the year of assessment. It is promptly updated if any significant new risks emerge or significant changes occur in existing risks, in operations or in the organisational or corporate structure.

In addition, an interim (half-yearly) self-assessment is carried out, according to the same methodology, the results of which are assessed by the Board of Directors, after review by the Control and Risk Committee and the Board of Statutory Auditors.

Lastly, in the event of the opening of new lines of business, the anti-money laundering function conducts a self-assessment of the risks of money laundering and terrorist financing associated with them.

Annex 1 – INFORMATION FLOWS

INFORMATION FLOW	DESCRIPTION	SENDER	RECIPIENT	FREQUENCY
1. Annual report on operations	The AML function prepares and submits a report which explains: the activities carried out by it in compliance with the approved activity plan; updates on the regulations that occurred during the period, the interventions carried out, follow-ups and suggested activities to prevent or mitigate the risk of money laundering or financing of terrorism; the results of the self-assessment on exposure to money laundering risk; a summary of training activities on anti-money laundering carried out during the year and the training plan for the following year; planning of the activities to be carried out during the following financial year	Parent Company's AML function	• Board of Directors • Control and Risks Committee • Board of Statutory Auditors • Internal Audit Department • Risk Control Unit	Annual
2. Interim report on operations	The AML function prepares and submits a summary and/or details of the results of the activities performed during the six-month period, their progress with respect to the annual planning, in addition to reporting the dysfunctions detected in the verification activities and the outcome of interim the self-assessment	Parent Company's AML function	• Board of Directors • Risk and Control Committee • Board of Statutory Auditors • Internal Audit Department • Risk Control Unit	Half yearly
3. Reports of anomalies and infringements	The AML function promptly informs the corporate bodies of significant violations or deficiencies found in the performance of the related tasks and of infringements pursuant to art. 46, para. 1,b) and of art. 51, paragraph 1 of Legislative Decree 231/2007, for subsequent communication to the Supervisory Authority or the MEF	Parent Company's AML function	• Board of Directors • Control and Risks Committee • Board of Statutory Auditors • Supervisory Body	Event by event
4. Information on specific requests from the Supervisory Authorities	The AML function prepares specific information when requests are received from the Supervisory Authorities	Parent Company's AML function	• Board of Directors • Board of Statutory Auditors	Event by event
5. Evaluation of the risks associated with entering new markets, launching new activities and innovative new products/services	The AML function assesses in advance the money laundering risk associated with the provision of new products and services	Parent Company's AML function	• Managing Director	Event by event
6. Audit reports	The internal audit department prepares and submits the results of its checks in which irregularities or defaults have been found in the structures controlling the risk of money laundering and financing of terrorism, also at banking Group level	Internal Audit Department	Parent Company's AML function	Event by event
7. Annual report on operations	The subsidiary's anti-money laundering function prepares and submits a report outlining: the planning of activities to be carried out during the next financial year and carried out by the subsidiary in	Subsidiary's AML function	Parent Company's AML function	Annual

INFORMATION FLOW	DESCRIPTION	SENDER	RECIPIENT	FREQUENCY
	accordance with the approved plan of activities; updates on legislation during the period, actions taken, follow-ups and suggested activities to prevent or mitigate the risk of money laundering or terrorist financing; the results of the self-assessment exercise on the exposure to money laundering risk; a summary of the anti-money laundering training and education activities carried out during the year and the training plan for the next financial year			
8. Interim report on operations	The subsidiary's anti-money laundering function prepares and submits a summary and/or detailed report of the results of the activities carried out during the period, the progress of the activities with respect to the annual planning, as well as the reporting of the dysfunctions detected in the audit activities and the results of the intermediate self-assessment	Subsidiary's AML function	Parent Company's AML function	Half-yearly
9. Reporting of anomalies	The anti-money laundering function of the subsidiary prepares and submits a report on significant breaches or deficiencies found in the performance of its duties.	Subsidiary's AML function	Parent Company's AML function	Event by event