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 terrorist financing of Banca Popolare di Sondrio and the Banking Group Banca Popolare di Sondrio

Identification code:	DDI_066_E2_15032024
Issuing unit:	Group Anti-Money Laundering Service
Approved by:	Board of Directors
Edition:	E2
Revision date:	15/03/2024
Circulation regime:	PUBLIC

Document versions

Date	Version	Description
06/2023	E1	First Edition
03/2024	E2	- General update in implementation of the Bank of Italy's new *Provisions on Organisation, Procedures and Internal Controls to Prevent the Use of Intermediaries for the Purposes of Money Laundering and Terrorist Financing,* as amended by Order of 1 August 2023 (effective from 15 November 2023); in particular, Introduction of the figure of the Anti-Money Laundering Officer; - Integration of paragraph 3.1 with the express indication of the figure of the *Compliance officer* at the Monte Carlo branch of Banca Popolare di Sondrio SUISSE; - Acknowledgement of the amendments to Legislative Decree No. 231/2007, which took place following the publication of Law No. 136 of 9 October 2023, '*Conversion into law, with amendments, of Decree-Law No. 104 of 10 August 2023, setting out urgent provisions for the protection of users, economic and financial activities and strategic investments*'. *104, containing urgent provisions to protect users, concerning economic and financial activities and strategic investments*', implementing the provisions of the *Guidelines on Policies and Controls for the Effective Management of Money Laundering and Terrorist Financing Risks in Providing Access to Financial Services,* published by the *European Banking Authority* (EBA/GL/2023/04), in force since 3 November 2023.

Approval of the document

Prepared by:	**Group Anti-Money Laundering Service**		**04/03/2024**
		[Constantine Tornadù]	**Date**
Validated by:	**Managing Director**		**07/03/2024**
		[Mario Alberto Pedranzini]	**Date**
Approved by:	**Board of Directors**		**15/03/2024**
		[Resolution of approval]	**Date**

INDEX

1. INTRODUCTION, REGULATORY FRAMEWORK AND OBJECTIVES

1.1. Introduction

Money laundering and terrorist financing are criminal phenomena that, also because of their possible transnational dimension, pose a serious threat to the economy and can have destabilising effects, especially on the banking and financial system.

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

The changing nature of the threats of money laundering and terrorist financing, also facilitated by the continuous evolution of technology, requires constant adaptation of prevention and countermeasures.

The recommendations of the Financial Action Task Force on Money Laundering and Terrorist Financing (hereinafter also referred to as 'FATF'), the main international coordinating body on the subject, require public authorities and the private sector to identify and assess the money laundering and terrorist financing risks to which they are exposed, in order to take appropriate mitigation measures.

Action to prevent and combat money laundering (hereinafter also AML) and the financing of terrorism (hereinafter also CTF or CFT) is carried out through the introduction of controls aimed at ensuring full knowledge of the customer, the traceability of financial transactions and the identification of suspicious transactions.

The intensity of the prevention and countermeasures must be modulated according to a *risk-based approach*, focused on the hypotheses deserving greater investigation and implemented by making monitoring activities more effective and efficient. This approach is the cornerstone for the prevention activity of the obliged parties and for the control action of the competent Supervisory Authorities.

Banca Popolare di Sondrio (hereinafter also referred to as the "bank" or the "Parent Company") and the companies of the Banking Group are strongly committed to preventing the products and services offered from being used for the purposes of money laundering and terrorist financing, promoting a culture of full compliance with the provisions in force and the effective fulfilment of the obligations of passive cooperation, aimed at ensuring a thorough knowledge of customers, the preservation of documents relating to transactions carried out, and active cooperation aimed at identifying and reporting suspicious money laundering operations. For this reason, the bank and the companies in the Banking Group have adopted this *policy* (hereinafter also referred to as the 'Document') at a general level as an expression of their commitment to combating the aforementioned criminal phenomena.

The bank is absolutely committed to ensuring that its operational organisation and control system is complete, adequate, functional and reliable, in order to protect the bank and the Banking Group from any conduct, even unconscious, of tolerance or admixture towards forms of illegality that may damage its reputation and jeopardise its stability. For these reasons, the bank and the Banking Group have adopted organisational and behavioural rules and monitoring and control systems aimed at ensuring compliance with current legislation by the administrative and control bodies, staff, collaborators and consultants of the Banking Group companies.

1.2. Anti-Money Laundering and Countering the Financing of Terrorism Regulatory Framework

Anti-money laundering and counter-terrorist financing legislation is contained in a complex and articulated system of sources at international, EU and national level.

At the international level, a fundamental contribution to the process of legislative harmonisation is provided by the FATF, the main body active in the fight against money laundering, terrorist financing and the proliferation of weapons of mass destruction. The body has prepared a set of *standards*, the so-called '40 Recommendations', adopted in February 2012 and constantly updated, accompanied by '9 Special Recommendations' and 'Interpretative Notes'.

At the European level, the relevant regulations are contained in Directive (EU) 2015/849 of the European Parliament and of the Council (hereinafter also "IV Directive"), of 20 May 2015, which repealed Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, followed by Directive (EU) 2018/843 of the European Parliament and of the Council (the "V Directive"), dated 30 May 2018, which, in amending the previous Directive, also included providers of foreign exchange services between virtual currencies and legal tender currencies and providers of digital wallet services among the addressees.

The following regulation is also relevant in this context:

- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds;
- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016, as amended and supplemented, supplementing Directive IV by identifying high-risk third countries with strategic shortcomings;
- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and establishing minimum rules relating to the definition of criminal offences and sanctions in the field of terrorist offences;
- Commission Delegated Regulation (EU) 2018/1108 of 7 May 2018 supplementing the Fourth 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 on their functions;
- Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls of cash entering or leaving the European Union;

- Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by means of criminal law and establishing minimum rules concerning the definition of criminal offences and sanctions in the field of money laundering;
- Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the recognition and execution within the European Union of freezing and confiscation orders issued by another Member State in the framework of proceedings in criminal matters;
- Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for minimum action and the type of additional measures to be taken by credit and financial institutions to mitigate the risk of money laundering and terrorist financing in certain third countries.

In addition to the primary regulations, there are also the guidelines that the *European Banking Authority (*EBA) periodically publishes, implemented in Italy following a declaration of compliance by the Bank of Italy, among which the following are worth mentioning in particular

- *Guidelines pursuant to Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence measures and factors that credit and financial institutions should take into account when assessing the money laundering and terrorist financing risks associated with individual ongoing relationships and occasional transactions ("ML/TF Risk Factor Guidelines")*, repealing and replacing JC/2017/37, dated 1 March 2021;
- *Guidelines on policies and procedures relating to compliance management and the role and responsibilities of the AML officer pursuant to Article 8 and Chapter VI of Directive (EU) 2015/849* published by the EBA on 14 June 2022.

At the national level, the legislative framework is represented by Legislative Decree No. 231 of 21 November 2007, as amended and supplemented, and Legislative Decree No. 109 of 22 June 2007, as amended and supplemented.

These regulations are supplemented by the provisions of the competent Supervisory Authorities aimed at fully implementing the anti-money laundering and counter-terrorist financing regulations defined at primary level. In particular, they point out:

- "Bank of Italy 'Provisions on organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing';
- "Bank of Italy 'Customer Due Diligence Provisions for Combating Money Laundering and Terrorist Financing';
- "Bank of Italy 'Provisions for the storage and provision of documents, data and information to combat money laundering and terrorist financing';
- 'Instructions on objective communications' of the Financial Intelligence Unit;
- "Provisions for sending aggregated data" of the Financial Intelligence Unit;
- "Supervisory Provisions on Sanctions and Administrative Sanctioning Procedure" of the Bank of Italy.

In addition to these provisions, which are of a secondary nature, are the measures and communications of the Bank of Italy and the FIU containing anomaly indicators and patterns of abnormal behaviour.

1.3. Legal framework on embargoes and international financial sanctions

The UN Charter empowers the UN Security Council to decide, in a manner binding on all members, on restrictive measures designed to promote the maintenance or restoration of international peace and security. The Treaty on European Union and the Treaty on the Functioning of the European Union provide for member states to take a common position in interrupting or restricting economic and financial relations with one or more third countries. These measures, which may be imposed against sovereign states, regimes, individual terrorists, terrorist organisations, and producers and disseminators of weapons of mass destruction, are aimed at:

- to safeguard the common values, fundamental interests, independence and integrity of the European Union in accordance with the principles contained in the UN Charter;
- strengthen the security of the European Union;
- preserve peace and strengthen international security;
- promote international cooperation;
- developing and consolidating democracy, respect for the law, human rights and fundamental freedoms.

The reference legislation for handling embargoes can be divided into the following categories:

- UN Security Council resolutions;
- European regulations;
- national primary and secondary legislation.

The main legislation issued by the UN is contained in the following sources:

- Resolutions adopted by the Security Council under Article 41 of Chapter VII of the UN Charter, by which restrictive measures are imposed on individuals and/or countries.

The main European legislation is contained in the following measures:

- Council Regulation (EC) 2580/2001 of 27 December 2001 imposing a freezing of funds and a prohibition on providing financial services to certain natural persons, legal persons, groups or entities committing or attempting to commit acts of terrorism and to legal persons, groups or entities controlled by them;
- Council Regulation (EC) 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities (listed in the Annex to the Regulation) associated with Usama bin Laden, the Al-Qaida network and the Taliban;
- Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

There are also other sources originating from the international and European context that establish a particular regime of prohibition to invest in certain industries or to import/export from/to certain countries, which are constantly updated.

Italian primary legislation is contained in the following provisions:

- Law No 185 of 9 July 1990, as amended and supplemented, containing new regulations on the control of the export, import and transit of armament materials;
- Legislative Decree No. 221 of 15 December 2017, as amended and supplemented, which reorganised and simplified the regulation of export authorisation procedures for dual-use items and technologies and trade embargo sanctions, as well as for all types of export transactions of proliferating materials[1] .

The main secondary legislation is contained in the following regulatory source issued by the Bank of Italy:

- Provision of 27 May 2009 on operational guidance for the exercise of enhanced controls against the financing of WMD proliferation programmes.

Also of relevance are the regulations issued by the US Authorities, contained - in addition to the *US Patriot Act*[2] - in the economic and trade sanctions decided from time to time by the US Government, through the *Office of Foreign Asset Control* ('OFAC'), as part of foreign policy and national security choices.

The regulatory framework of reference, which has correlations with that on combating money laundering and the financing of terrorism, provides for restrictive measures and sanctions against both governments of third countries and non-state entities, natural persons or legal entities in the area of

- arms embargoes;
- other specific or general trade restrictions (export and import bans);
- financial restrictions (freezing of assets and resources, bans 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 *dual-use* regulations.

[1] The regulations previously contained in Legislative Decree No. 96 of 9 April 2003, Legislative Decree No. 11 of 12 January 2007, and Legislative Decree No. 64 of 14 May 2009, which have been repealed, were incorporated into this decree.

[2] *US Patriot Act* (*Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism* - 2001) which, enacted in the aftermath of the 11 September 2001 terrorist attacks, extended the requirements of the *Bank Secrecy Act* ('BSA' - 1970), requiring financial institutions to prepare *due diligence* procedures and improving information sharing between financial institutions and the US Government.

1.4. Purpose

This Document is drafted in accordance with Articles 15 and 16 of Legislative Decree 231/2007, with the "Provisions on the organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing", the "Provisions on customer due diligence for combating money laundering and terrorist financing", the 'Provisions on the storage and provision of documents, data and information for the purpose of combating money laundering and terrorist financing', issued by the Bank of Italy and the FIU, and the 'Guidelines on policies and procedures relating to compliance management and the role and responsibilities of the AML officer' issued by the EBA. The same defines the guidelines relating to the AML/CFT risk management system of the Parent Company and the Banking Group, in terms of:

- general principles of the risk management model and strategic orientations;
- responsibilities and tasks of the corporate bodies and corporate structures of both the parent company and the subsidiaries;
- operating procedures for the management of the risk of money laundering and terrorist financing in the context of due diligence, for *the on-boarding of* high-risk customers, for the storage and provision of documents, data and information and for the reporting of suspicious transactions, reasonably homogeneous at Group level;
- sharing among the various Group companies, subject to the regulatory constraints existing in foreign jurisdictions, of information useful for assessing the money laundering and terrorist financing risks to which the Banking Group is exposed.

1.5. Responsibility and entry into force of the Document

This Document is approved by the Board of Directors of Banca Popolare di Sondrio, after consulting the Board of Statutory Auditors and is addressed to all employees and collaborators of the bank and its subsidiaries Banca della Nuova Terra Spa, Factorit Spa and Banca Popolare di Sondrio (SUISSE) SA.

The Document is revised at least every two years and, in any case, following significant changes in the reference legislation, the organisational and governance structures of the Banking Group and the operations carried out by the individual companies.

All significant amendments and/or additions to the Document are approved by the bank's Board of Directors, after consulting the Board of Statutory Auditors. If the adjustments are merely reconnaissance of board resolutions or organisational revisions that have taken place, as well as in the case of further amendments of a purely formal nature, the approval is referred to the Managing Director.

Without prejudice to the Board of Directors' authority to approve any relevant amendments and/or additions to the Document, its update and periodic review are prepared by the bank's anti-money laundering structure and subsequently validated by the Managing Director.

Prior to its approval, the Document is submitted to the Control and Risk Committee for its evaluations.

The *policy* or its amendments enter into force on the first day of the month following the month of approval.

1.6. Addressees of the Document

The Head of the Group Anti-Money Laundering Service is entrusted with the task of disseminating this *policy* to the Banking Group companies for subsequent approval, in accordance with a principle of proportionality and taking into account local regulations and specificities, by the relevant Bodies with strategic supervisory functions, on the basis of the following scope of application:

- to all Italian companies subject to anti-money laundering and anti-terrorist financing provisions;
- to banks belonging to the banking group based abroad, in compliance with and compatible with local regulations.

The subsidiaries of the Banking Group shall inform the Parent Company of the outcome of the transposition process of this Document in the manner provided for in the 'Management of Corporate Rules and Regulations' of 30 June 2023 .

The Document is also made available and easily accessible to all employees and collaborators, both of the bank and of the banking group companies, including by means of publication on their respective corporate *intranets*.

The transposition of the guidelines and principles contained in this *policy* at the Banking Group level is preparatory to fostering adequate coordination between local AML/CFT units and the Group AML department and to ensuring an effective circulation of information at Group level, in order to counter the risk of money laundering and terrorist financing.

1.7. Definitions and acronyms

- "*Senior manager*": a Director or the General Manager or other employee delegated by the Management Body or the General Manager to deal with high-risk customers; the senior manager has appropriate knowledge of the level of risk of money laundering or terrorist financing to which the recipient is exposed and is endowed with a sufficient degree of autonomy to take decisions capable of affecting this level of risk;
- '*AML*': acronym, commonly used internationally, for Anti *Money* Laundering;
- "*Standardised archives*": archives by means of which the data and information provided for in the Bank of Italy's "Provisions for the storage and making available of documents, data and information for combating money laundering and the financing of terrorism" are stored and made available; they include the single computer archives already established on the date of entry into force of Legislative Decree No 90 of 25 May 2017;

- "*Sector Supervisory Authorities" means* the Bank of Italy, CONSOB and IVASS as national authorities in charge of the supervision and control of banking and financial intermediaries and *the European Banking Authority;*
- *"shell bank" means a* bank or institution performing similar functions to a bank that does not have a significant organic and managerial structure in the country in which it is incorporated and authorised to carry on business, nor is it part of a financial group subject to effective supervision on a consolidated basis;
- *"Customer":* the person who establishes or has ongoing relations or carries out occasional transactions; in the case of ongoing relations or occasional transactions co-owned by several persons, each of the co-owners is deemed to be a customer;
- *"Freezing of funds" means* the prohibition, under Community regulations and national law, of the movement, transfer, alteration, use or management of funds or access to them, so as to change their volume, amount, location, ownership, possession, nature, destination or any other change that enables the use of funds, including *portfolio* management*;*
- *"Freezing of economic resources" means* the prohibition, under EU regulations and national law, of the transfer, disposition or, for the purpose of obtaining funds, goods or services in any manner whatsoever, use of economic resources, including, but not limited to, the sale, lease, rental or pledging of security interests;
- *"Correspondent accounts and similar" means* accounts held by banks for the settlement of interbank services, used for the settlement of transactions on behalf of customers of correspondent institutions;
- "*Transfer accounts":* cross-border correspondent banking relationships between banks and financial intermediaries used to carry out transactions in their own name and on behalf of their customers;
- *"Line controls":* controls carried out by the operational structures (e.g. hierarchical, systematic and spot checks), also through units dedicated exclusively to control tasks reporting to the heads of the operational structures, or carried out as part of the *back office*, incorporated in the IT procedures and aimed at ensuring the proper performance of operations;
- *"Risk and compliance controls": these* aim to ensure, inter alia:
  - the proper implementation of the risk management process;
  - compliance with the operational limits assigned to the various functions;
  - compliance of company operations with standards, including self-regulatory ones;
- '*CTF*': acronym, commonly used internationally, for *Counter* Terrorism Financing, i.e. preventing the financing of terrorism; alternatively, the acronym CFT - *Combating the Financing of Terrorism* - is also used;
- *"Identification data" means* the first name and surname, the place and date of birth, the registered residence and domicile, if different from the registered residence, and, where assigned, the tax code or, in the case of entities other than natural persons, the name, registered office and, where assigned, the tax code*;*

- *"Anti-Money Laundering Decree":* Legislative Decree No. 231 of 21 November 2007, as amended and supplemented;
- *'Anti-Terrorism Decree':* Legislative Decree No. 109 of 22 June 2007, as amended and supplemented;
- *"Delegate for reporting suspicious transactions":* the person designated by Banca Popolare di Sondrio "s Body with strategic supervisory functions to assess suspicious transactions and to subsequently transmit them to the Financial Intelligence Unit, if deemed grounded;
- *"Cash" means* banknotes and coins, in euro or in foreign currencies, which are legal tender;
- *"Anti-Money Laundering Directive" means* the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC , as amended by Directive (EU) 2018/843, of the European Parliament and of the Council, of 30 May 2018 *;*
- *'Embargo': a* ban on trade and commerce with sanctioned countries, aimed at isolating and placing their government in a difficult domestic political and economic situation;
- *"Executor":* the person delegated to act in the name and on behalf of the customer or who is otherwise vested with powers of representation enabling him to act in the name and on behalf of the customer;
- *"Anti-Money Laundering Officer":* is appointed by the Board of Directors from among its members; constitutes the main point of contact between the Group Anti-Money Laundering Officer, the Board of Directors and the Managing Director in his capacity as Management Body. He also ensures that the same Bodies have the necessary information to fully understand the significance of the money laundering risks to which the bank is exposed, for the purpose of exercising their respective powers;
- *"Officer in charge of the Group Anti-Money Laundering* service*":* he is appointed by the Board of Directors of the Parent Company from among its members and may coincide with the officer in charge of the anti-money laundering of Banca Popolare di Sondrio; he is the main point of contact between the officer in charge of the Group Anti-Money Laundering service, the Bodies with strategic supervisory and management functions of the Parent Company and ensures that the latter have the necessary information to fully understand the significance of the money laundering risks to which the Group is exposed, for the purposes of exercising their respective powers. He also ensures that the Group Anti-Money Laundering Officer carries out his duties effectively;
- *"Terrorist financing":* for the purposes of Legislative Decree 109/2007, as amended, financing of terrorism shall mean any activity aimed, by any means, at the supply, collection, provision, intermediation, deposit, custody or disbursement of funds and economic resources, howsoever carried out, intended to be used, directly or indirectly, in whole or in part, for the commission of one or more forms of conduct for the purposes of terrorism, in accordance

with the provisions of the criminal laws, regardless of the actual use of the funds and economic resources for the commission of the aforesaid conduct;

- *"Funds":* financial assets and benefits of every kind, including income derived therefrom, owned, held or controlled, even partially, directly or indirectly, or through nominees, or by natural or legal persons acting on their behalf or at their direction (such as cash cheques, pecuniary credits, bills of exchange, payment orders and other payment instruments, deposits with financial institutions or other entities, balances on accounts, receivables and bonds of any kind, negotiable securities in the public and private sectors, financial instruments as defined in Legislative Decree no. 58 of 24 February 1998, interest, dividends or other income and increases in value generated by assets, credit, right of set-off, guarantees of any kind, sureties and other financial commitments, letters of credit, bills of lading and other securities representing goods, documents evidencing an interest in funds or financial resources, all other instruments of export financing, life insurance policies, etc.);
- *"Company control functions":* the set of functions that, by legislative, regulatory, statutory or self-regulatory provision, have control tasks. At Banca Popolare di Sondrio, these functions coincide with the Compliance Function, the Group Anti-Money Laundering Service, the Risk Control Service and the Internal Audit Service;
- *"Banking Group":* the Banca Popolare di Sondrio Banking Group pursuant to Article 60 et seq. of Legislative Decree No. 385 of September 1, 1993 ("Consolidated Banking Act" or "TUB"), as amended and supplemented, consisting of the Parent Company and its subsidiaries;
- *"Community banking and financial intermediaries" means* the entities referred to in Article 3(1) and (2) of the "Anti-Money Laundering Directive" having their head office in an EU country;
- *"Means of payment" means* cash, bank and postal cheques, bankers' drafts and other cheques assimilated or equivalent to them, money orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, pledge policies and any other instrument available to transfer, move or acquire, including by telematic means, funds, securities or financial assets;
- *"Transaction" shall mean the* activity consisting in the movement, transfer or transmission of means of payment or in the performance of acts of negotiation having a financial content; the conclusion of an act of negotiation, having a financial content, falling within the scope of professional or commercial activity also constitutes a transaction;
- *"Fractional transaction":* a unitary transaction in terms of economic value, of an amount equal to or greater than the limits laid down in the anti-money laundering decree, carried out by means of several transactions, each of which is lower than the aforesaid limits, carried out at different times and within a limited period of time fixed at seven days, without prejudice to the existence of a fractional transaction when there are elements to consider it as such;
- *"Occasional transaction":* a transaction that is not part of an ongoing relationship; an intellectual or commercial service, including those with instantaneous performance, rendered in favour of the customer also constitutes an occasional transaction;

- *"Suspicious transaction":* a transaction which, on account of its characteristics, size, nature and connection with other transactions or its splitting up or any other circumstance known by reason of the functions performed, taking into account also the economic capacity and the activity carried on by the person to whom it relates, on the basis of the elements acquired pursuant to the anti-money laundering decree, leads to the belief, suspicion or reasonable grounds for suspecting that money laundering or terrorist financing operations are being or have been carried out or attempted, or that the funds, regardless of their size, originate from criminal activity;
- *"Connected transactions":* transactions that are connected with each other in pursuit of a single objective of a capital legal nature;
- *"Corporate bodies":* the set of bodies with strategic supervision, management and control functions*;*
- *"Supervisory Body":* the Body established pursuant to Legislative Decree No. 231 of 8 June 2001;
- *"Body with control function":* the corporate body responsible, among other things, for supervising the completeness, adequacy, functionality and reliability of the internal control system. At Banca Popolare di Sondrio, the Body with control functions is represented by the Board of Statutory Auditors;
- *"Body with management function":* the corporate body or its members to which management tasks are assigned or delegated, i.e. the implementation of the policies resolved upon in the exercise of the strategic supervision function. At Banca Popolare di Sondrio, this body is represented by the Managing Director;
- *"Body with strategic supervision function":* the Body in which the functions of policy-making and/or supervision of corporate management are concentrated (e.g.: by means of examination and resolution on the Company's industrial and/or financial plans and/or strategic transactions). At Banca Popolare di Sondrio, the Strategic Supervision Body is represented by the Board of Directors;
- "*Community countries*" means countries belonging to the European Economic Area;
- *"Third countries" means* countries outside the European Economic Area;
- *"High-risk third countries":* countries outside the European Economic Area whose systems have strategic deficiencies in their national AML/CFT regimes, as identified by the European Commission in the exercise of its powers under Articles 9 and 64 of the AML Directive;
- *"Personnel":* employees and those who in any case work on the basis of relationships that lead to their inclusion in the organisation of the obliged party, also in a form other than an employment relationship;
- *"Politically exposed persons" (or PEPs):* natural persons who hold or have held for less than one year important public office, their family members and those known to have close ties with the above-mentioned persons, as listed below:
  - natural persons who hold or have held important public office are those who hold or

have held the office of:

- President of the Republic, President of the Council, Minister, Vice-Minister and Under-Secretary, President of the Region, 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 States;
- deputy, senator, member of the European Parliament, regional councillor and similar offices in foreign states;
- member of the central governing bodies of political parties;
- judge of the Constitutional Court, magistrate of the Court of Cassation or of the Court of Auditors, councillor of State and other members of the Council of Administrative Justice for the Sicilian Region and similar positions in foreign states;
- member of the governing bodies of central banks and independent authorities;
- ambassador, chargé d'affaires or equivalent positions in foreign states, senior officer in the armed forces or similar positions in foreign states;
- members of the administrative, management or supervisory bodies of undertakings controlled, even indirectly, by the Italian State or a foreign State or in which the Regions, provincial capitals and metropolitan cities and municipalities with a total population of not less than 15,000 inhabitants hold a majority or full stake;
- general manager of ASLs, hospital companies, university hospitals and other bodies of the national health service;
- director, deputy director and member of the management body or person performing equivalent functions in international organisations;

- The following are family members of politically exposed persons: the parents, spouse or person bound to the politically exposed person in a civil partnership or de facto cohabitation or comparable institutions, children and their spouses and persons bound to the children in a civil partnership or de facto cohabitation or comparable institutions;
- are individuals with whom politically exposed persons are known to have close ties:
  - natural persons who, within the meaning of the Anti-Money Laundering 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 have been set up, de facto, in the interest and for the benefit of a politically exposed person;

- *"Local Italian Politicians" (or PILs)*: persons who, although not PEPs, operate in contexts closely related to local political life and who, therefore, present a higher potential risk of money laundering, identified by the bank in the following figures: provincial president, provincial councillor and municipal councillor, mayor of municipalities with a population of less than 15,000 inhabitants;

- *"Trust and company service providers" means* any natural or legal person who provides third parties, in a professional capacity, with any of the following services:
  - set up companies or other legal persons;
  - occupying the function of an officer or director of a company, a member of an association or a similar function in relation to other legal persons or arranging for another person to occupy such a function;
  - provide a registered office, business, administrative or postal address and other related services to a company, association or any other legal entity;
  - perform the function of a trustee in an express *trust or* similar legal arrangement or arrange for another person to perform that function;
  - exercising the role of shareholder on behalf of another person or arranging for another person to perform that function, provided that the company is not a company listed on a regulated market and subject to disclosure requirements in accordance with European Union or equivalent international standards;
- *" Providers of services related to the use of virtual currency* ": any natural person or legal entity that provides third parties, on a professional basis, including *online*, with services functional to the use, exchange, storage of virtual currencies and their 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 functional to the acquisition, trading or intermediation in the exchange of the same currencies;
- *" Digital Wallet Service Providers* ": any natural or legal person who provides third parties, on a professional basis, including *online, with* private cryptographic key protection services on behalf of its clients, in order to hold, store and transfer virtual currencies;
- *"Accounts similar to pass-through accounts" shall mean* those accounts, however denominated, held between banking and financial intermediaries over which the customer of the correspondent institution is given the authority to execute directly even only part of the transactions pertaining to it;
- *"Continuous relationship" means* a relationship of duration, forming part of the establishment activity carried out by the obliged parties, which does not end in a single transaction*;*
- *"Correspondent* banking *relationships" means* accounts held by banks for the settlement of interbank services (remittances of bills, bank and bank cheques, deposit orders, transfers of funds, documented remittances and other transactions) as well as relationships, however denominated, held between banking and financial intermediaries used for the settlement of transactions on behalf of the respondent institutions' customers (e.g. securities deposits, investment services, foreign exchange transactions, document collection services, issuance or management of debit or credit cards);
- *"Money laundering":* for the purposes of Legislative Decree 231/2007 as amended, money laundering means:

- the conversion or transfer of property, carried out in the knowledge that such property is derived from criminal activity or from participation in such activity, for the purpose of concealing or disguising the illicit origin of such property or of assisting any person involved in such activity to evade the legal consequences of his or her actions;
- concealment or disguise of the true nature, source, location, disposition, movement, ownership of property or rights thereto, carried out in the knowledge that such property is derived from criminal activity or from participation in such activity;
- the purchase, possession or use of goods in the knowledge, at the time of their receipt, that they originate from criminal activity or from participation in such activity;
- participation in one of the acts referred to in the preceding paragraphs, association to commit such an act, attempt to commit such an act, aiding, abetting, instigating or counselling someone to commit such an act, or facilitating the commission of such an act.

Self-laundering also falls under this definition, where the launderer is the same as the perpetrator of the predicate offence;

- *"Money Laundering and Terrorist Financing Risk":* the risk arising from the breach of statutory, regulatory and self-regulatory provisions aimed at preventing the use of the financial system for the purpose of money laundering, terrorist financing or the financing of programmes for the development of weapons of mass destruction;
- *"Risk Appetite Framework":* the reference framework that defines - consistently with the maximum risk that can be assumed, the *business model* and the strategic plan - the risk appetite, the tolerance thresholds, the risk limits, the risk governance policies, and the reference processes necessary to define and implement them;
- *"Economic resources" means* assets of every kind, whether tangible or intangible, and movable or immovable property, including accessories, appurtenances and fruits, which are not funds but which may be used to obtain funds, goods or services, owned, held or controlled, even partially, directly or indirectly, or through intermediaries, by designated persons, or by natural or legal persons acting on behalf of or at the direction of such persons;
- *"System of internal controls":* the set of rules, functions, structures, resources, processes and procedures that aim to ensure, in compliance with sound and prudent management, the following purposes:
  - verification of the implementation of company strategies and policies;
  - containment of risk within the limits specified in the framework for determining the bank's risk appetite;
  - preservation of asset value and protection against losses;
  - effectiveness and efficiency of business processes;
  - reliability and security of company information and IT procedures;
  - prevention of the risk of the bank being involved, even unintentionally, in unlawful activities (with particular reference to those connected with money laundering, usury and

terrorist financing);

- compliance of transactions with the law and supervisory regulations, internal policies, regulations and procedures;

- *"Designated persons" means* natural persons, legal persons, groups and entities designated as recipients of freezing on the basis of EU regulations, UN resolutions and national legislation;
- *"Operational Structures": the* bank "s territorial branches; they represent the first and essential level of corporate supervision for the purposes of preventing and combating money-laundering and terrorist financing phenomena, and are concretely responsible for the administration and management of relations with customers;
- *'beneficial owner*':
  - the natural person or persons on whose behalf the customer establishes an ongoing relationship or carries out a transaction (in short, 'beneficial owner *sub* 1');
  - where the customer and/or the entity on whose behalf the customer establishes an ongoing relationship or enters into a transaction are entities other than a natural person, the natural person(s) who ultimately has direct or indirect ownership of the entity or control over it or who is (are) its beneficiary(ies) (in short, "beneficial owner *sub* 2)"). In particular, in the case of corporations or other private legal entities, even if based abroad, and express *trusts,* irrespective of their place of establishment and the law applicable to them, the beneficial owner *sub* 2) is identified in accordance with the criteria set out in Articles 20 and 22(5) of Legislative Decree 231/2007; the same criteria apply, mutatis mutandis, in the case of partnerships and other legal entities, public or private, even if without legal personality;
- *"Bearer security" means a security* entitling the holder to exercise the right mentioned therein by mere presentation and the transfer of which is effected by delivery of the security;
- 'FIU': the Financial Intelligence Unit for Italy, established at the Bank of Italy;
- *"Virtual currency" means a* digital representation of value, not issued or guaranteed by a central bank or public authority, not necessarily linked to a legal tender, used as a medium of exchange for the purchase of goods and services or for investment purposes and transferred, stored and traded electronically.

2. ROLES AND RESPONSIBILITIES OF BODIES, FUNCTIONS AND CORPORATE STRUCTURES

2.1. Body with Strategic Supervisory Function (OFSS)

The OFSS, that is, the Board of Directors, approves and periodically reviews the strategic direction and policies for the governance of money laundering and terrorist financing risks and is responsible for oversight and implementation within the bank's *governance* and internal control framework. The OFSS must collectively possess adequate knowledge, skills and experience to understand the money laundering and terrorist financing risks related to the bank's activities and *business* model, including knowledge of the relevant legal and regulatory framework.

In this context, the Board of Directors:

- approves a specific anti-money laundering *policy*, which illustrates and justifies the choices that the bank and the Group intend to make on the various relevant profiles of organisational structures, procedures and internal controls, as well as on customer due diligence and data retention in order to assess consistency with actual exposure to money laundering risk;
- approves the guidelines of the internal control system, organic and coordinated, functional for the detection and management of money laundering risk and ensures its effectiveness over time;
- decides on the establishment, organisation, reconfiguration and/or abolition of the Group Anti-Money Laundering Service, identifying its tasks and responsibilities, as well as the methods of coordination with the other control functions and the anti-money laundering structures of the subsidiaries;
- approves the principles for managing relations with customers classified as 'high risk', specifying possible types of customers with whom the bank should not deal;
- resolves, after hearing the Body with control function, on the appointment and/or revocation of the person in charge of the anti-money laundering function of Banca Popolare di Sondrio and of his deputy; the verification of the possession of the requirements of the person in charge must be analytically reported in the appointment minutes;
- resolves, in consultation with the Controlling Body, on the appointment and/or dismissal of the Head of the Group Anti-Money Laundering Function and his deputy; the verification of the fulfilment of the requirements of the Head must be reported analytically in the minutes of the appointment;
- ensures the allocation of tasks and responsibilities in a clear and appropriate manner, guaranteeing the separation between operational structures and control functions;
- ensures an adequate, complete and timely information flow system towards the corporate bodies and between the control functions, as well as a documentation sharing system that

allows the corporate bodies direct access to the reports of the control functions on anti-money laundering matters, to the relevant communications with the Authorities and to the supervisory measures imposed or sanctions imposed;

- ensures the protection of the identity of the reporter of a suspicious transaction;
- at least twice a year, it examines the reports of the activity carried out by the Group Anti-Money Laundering Officer and the controls carried out by the competent functions, as well as the money laundering risk assessment document;
- assesses, at least once a year, the effective functioning of the Group Anti-Money Laundering service, taking into account, inter alia, the conclusions of any internal and external audits carried out, including with regard to the adequacy of the human and technical resources assigned to the head of the Group Anti-Money Laundering service, engaging the Personnel and Organisational Model Service for audits where appropriate;
- ensures that any anomalies or shortcomings found as a result of the second-level checks are immediately brought to its attention and that corrective measures are taken, the effectiveness of which it assesses;
- assesses the risks related to operations with third countries considered to be at 'high risk' of money laundering, identifies the safeguards to mitigate them and monitors their effectiveness;
- appoints the anti-money laundering officer of both the Parent Company and the Group, and ensures that they meet the conditions set out in the *Bank of Italy Provisions on Organisation, Procedures and Internal Controls for Anti-Money Laundering Purposes,* as well as Ministry of Economy and Finance Decree No. 169 of 23 November 2020[3] . The relevant assessments must be recorded in an analytical manner;
- ensures that the person appointed as the AML officer is promptly informed of decisions that may affect the bank's exposure to money laundering risk.

The OFSS has direct and timely access to the reports of the Group Anti-Money Laundering Officer and the Internal Audit Department, to the conclusions and observations of any external auditors in the AML/CFT area, as well as to the communications or findings of the competent authorities and any measures or sanctions imposed by them.

2.2. Representative responsible for anti-money laundering (of the bank and Group)

Without prejudice to the collective responsibility of the corporate bodies, the Board of Directors, while retaining responsibility for approving the bank's and the Group's overall AML/CTF strategy and overseeing its implementation, appoints one of its members as the AML/CTF officer. The appointment is of an executive nature.

[3] "*Regulation on the requirements and eligibility criteria for corporate officers of banks, financial intermediaries, confidiums, electronic money institutions, payment institutions and depositor guarantee schemes*".

The position of anti-money laundering officer may be attributed to a director without delegated powers (so-called non-executive director) who, as a result of such appointment, acquires the status of executive director and, as such, must comply with the suitability requirements laid down for such a role. It may also be attributed to the managing director; in any case, it is necessary to verify compliance with the requirements of the regulations and to consider possible situations of conflict of interest.

The anti-money laundering officer may not delegate his tasks to third parties.

This subject:

a) possesses adequate knowledge, skills and experience regarding money laundering risks, AML/CFT policies, controls and procedures, as well as the bank's *business* model and related area of operation;
b) has adequate time and resources to perform its tasks effectively.

The Anti-Money Laundering Officer is the main point of contact between the Group Anti-Money Laundering Officer, the Board of Directors and the Managing Director in his capacity as the body with management functions. He also ensures that these bodies have the necessary information to fully understand the significance of the money laundering risks to which the bank is exposed, for the purpose of exercising their respective powers.

When appointing the AML/CFT officer, the bank must identify and consider potential conflicts of interest and take measures to prevent or mitigate them. In any event, the provisions of the "*Regulation on the Control of the Independence Requirements of Directors*" approved by the Board of Directors on 19 January 2024 shall apply, including with respect to measures to prevent and mitigate conflicts of interest.

With regard to the verification of the availability of time necessary for the effective performance of the assignment, the provisions of Ministerial Decree No. 169 of 23 November 2020 ("*Regulation on the requirements and eligibility criteria for corporate officers of banks, financial intermediaries, confidiums, electronic money institutions, payment institutions and depositor guarantee schemes*") apply.

The person responsible for anti-money laundering:

a) monitors that AML policies, procedures and internal control measures are adequate and proportionate, taking into account the bank's characteristics and the ML/TF risks to which it is exposed;
b) assists the Board of Directors in evaluations concerning the organisational structure and resourcing of the Group Anti-Money Laundering Service, including the possible choice of assigning responsibility for this service to the same anti-money laundering officer;
c) ensures that corporate bodies are periodically informed of the activities carried out by the head of the Group Anti-Money Laundering Service, as well as of their contacts with the Authorities;
d) informs the corporate bodies of violations and critical issues concerning money laundering of which it has become aware and recommends appropriate action;

e) verifies that the Group Anti-Money Laundering Officer has direct access to all the information necessary to perform his duties, has sufficient human and technical resources and tools at his disposal, and is informed of any anti-money laundering deficiencies identified by the other internal control functions and the supervisory authorities;

f) ensures that the problems and proposals for action presented by the Head of the Group Anti-Money Laundering Service are assessed by the Managing Director.

Similarly, the Board of Directors of each Italian component of the Group to which the "Provisions on Organisation, Procedures and Internal Controls to Prevent the Use of Intermediaries for the Purposes of Money Laundering and Terrorist Financing" apply, appoints from among its members a person responsible for anti-money laundering, with similar procedures, requirements and duties to those mentioned above.

The Parent Company's Board of Directors also appoints a member as Group Money Laundering Officer, who must meet the same eligibility requirements as the Parent Company's Money Laundering Officer and may coincide with him. The duties of the Group Money Laundering Officer are set out in paragraph 3 below (*Banking Group's Money Laundering and Terrorism Financing Risk Management Model*).

2.3. Body with management function (OFG)

The OFG, in the person of the Managing Director:

- oversees the implementation of the strategic guidelines and money laundering risk governance policies approved by the Board of Directors and is responsible for the adoption of all measures necessary to ensure the effectiveness of the organisation and the system of anti-money laundering controls; to this end, it examines the proposals for organisational and procedural measures submitted by the head of the Group Anti-Money Laundering Department and formalises, giving reasons, any decision not to accept them;
- oversees the definition of a system of internal controls for the prompt detection and management of AML/CTF risk and ensures its effectiveness over time, consistent with the evidence drawn from the AML/CTF risk self-assessment exercise;
- ensures that operational procedures and information systems enable the proper fulfilment of customer due diligence and record-keeping obligations;
- with regard to the reporting of suspicious transactions, defines and ensures the implementation of a procedure suited to the bank's specific activities, size and complexity, which guarantees certainty of reference, uniformity of conduct, generalised application to the entire structure, full use of all relevant information and the traceability of the assessment process; it also adopts measures aimed at ensuring 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 the implementation of the initiatives and procedures necessary to ensure the timely fulfilment of reporting obligations to the Authorities under the anti-money laundering legislation;

- validates the anti-money laundering *policy* submitted to the Board of Directors for approval and ensures its implementation;
- defines information flows to ensure that all the company structures involved and the control bodies are aware of the risk factors;
- defines and oversees the implementation of procedures for managing relations with customers classified as 'high risk', consistent with the principles laid down by the Strategic Supervisory Board;
- establishes the appropriate tools to allow the verification of the activities carried out by staff in order to detect any anomalies that emerge, in particular, in their conduct, in the quality of communications addressed to contact persons and company structures and in staff relations with customers;
- ensures, in cases where the operational tasks of the anti-money laundering function are outsourced, compliance with the applicable regulations and receives regular information on the performance of the outsourced activities;
- ensures, in cases of remote operations, the adoption of specific IT procedures for compliance with anti-money laundering regulations, with particular reference to the automatic detection of anomalous transactions.

The Managing Director acts in cooperation with the Control and Risk Committee and reports to the Board of Directors on the initiatives and actions required to ensure the completeness, adequacy, functionality and reliability of the internal control and risk governance system on an ongoing basis.

In cooperation with the Group Anti-Money Laundering Service and the Personnel and Organisational Model Service, it establishes staff training and education programmes on AML obligations on a continuous and systematic basis.

2.4. Body with Control Functions (OFC)

The OFC, i.e. the Board of 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 Auditors:

- makes use of internal structures to carry out the necessary checks and verifications;
- uses information flows from other corporate bodies, the head of the Group Anti-Money Laundering Service and other corporate control functions;
- assesses the adequacy of the procedures for customer due diligence, document, data and information retention and suspicious transaction reporting;
- analyses the reasons for the deficiencies, anomalies and irregularities found and promotes the adoption of appropriate corrective measures.

He is also consulted on decisions to appoint the head of the Group Anti-Money Laundering Service, the deputy head of the Group Anti-Money Laundering Service, the person in charge of

suspicious transaction reports and the deputy head of STR, and in defining the elements of the overall architecture of the AML/CFT risk management and control system.

Pursuant to Article 46 of the Anti-Money Laundering Decree, the members of the Body with control functions shall report without delay to the Bank of Italy all facts of which they become aware in the course of their duties that may constitute serious or repeated or systematic or multiple violations of the applicable provisions of the law and of the relevant implementing provisions.

2.5. Supervisory body

The Supervisory Board (SB) established pursuant to Legislative Decree 231/01 continuously monitors compliance with the processes set out in the adopted Organisation, Management and Control Model.

If a predicate offence is nevertheless committed, it analyses its causes in order to identify the most suitable corrective measures. In order to carry out these activities, the Supervisory Board receives appropriate information flows from the various structures and/or functions of the company and has unrestricted access to all data and information relevant to the performance of its duties.

Finally, the Supervisory Board forwards to the STR manager any suspicious transaction reports it detects in the course of its duties.

2.6. Internal Audit Service

With regard to preventing and combating money laundering and terrorist financing, the Internal Audit Service is responsible for verifying the adequacy of the company's organisational set-up with respect to the relevant regulations, as well as supervising the functionality of the overall internal control system.

The Internal Audit Service periodically reviews the adequacy and effectiveness of the functions performed by the Group Anti-Money Laundering Service.

The service verifies, through systematic checks, including inspections:

- compliance with the duty of due diligence, both at the stage of establishing the relationship and as the relationship develops over time;
- the effective acquisition and orderly storage of documents, data and information;
- the degree of effective involvement of staff, as well as of the heads of central and peripheral structures, in the implementation of the communication and reporting obligation.

Interventions, both inspections and remote inspections, are planned according to a *risk-based* logic in order to allow the intensity of checks to be greater for the operational structures deemed most exposed to the risk of money laundering and terrorist financing, and for all operational structures to be assessed over a reasonable period of time.

It also carries out *follow up actions* to verify the adoption of the corrective measures envisaged for any anomalies detected, and reports, at least annually or as part of its periodic *reporting*, to

the corporate bodies on the activities carried out and their outcomes, subject to compliance with the confidentiality obligations laid down in the Anti-Money Laundering Decree.

Lastly, the head of the Parent Company's Internal Audit department supervises the activities of the Internal Audit functions present in the subsidiaries to ensure uniformity of controls and adequate attention to the different types of risk, including those attributable to non-compliance with the legal provisions on preventing and combating money laundering and terrorist financing.

2.7. Group Anti-Money Laundering Service

The Group Anti-Money Laundering Service is divided internally into:

- AML office of BPS;
- Group AML office.

The Group Anti-Money Laundering Service:

1) at least twice a year, prepare a Group-wide ML/TF risk assessment. In this regard, the Parent Company must take into account in its ML/TF risk management system both the individual risks of the various Group entities and their possible interrelationships, which could significantly affect the Group-wide risk exposure. Particular attention must be paid, in this context, to the risks to which Group companies established in third countries are exposed, particularly if they are at high ML/TF risk;
2) establishes AML/CTF policies and procedures, as well as the controls and systems to be applied pursuant to Article 8(4) of Directive (EU) 2015/849;
3) establishes AML/CFT *standards at* the Group level and ensures that local policies and procedures at the individual entity level comply with the AML/CFT laws and regulations applicable to each Group entity individually and are also in line with the *standards* established at the Group level;
4) defines Group-wide policies, procedures and measures concerning, in particular, data protection and information sharing within the Group for AML/CFT purposes, in accordance with national legal provisions;
5) Ensures that Group entities have adequate suspicious transaction reporting procedures in place and share information properly, including notification that a suspicious transaction report has been submitted (subject to limitations under national rules);
6) draws up and transmits to the Managing Director, the Board of Statutory Auditors, the *Chief Risk Officer* and the Head of Internal Audit specific Group indicators, useful for highlighting and monitoring the trend of the main money laundering and terrorist financing risk indicators, drawn up on the basis of the data provided by the individual Group members.

The Group Anti-Money Laundering Department reports - either directly or through the anti-money laundering officer - to the Board of Directors, the Managing Director, the Board of Auditors and has access to all the bank's activities, as well as to any information relevant to the performance of its duties.

Personnel called upon to collaborate in the Group Anti-Money Laundering Service, even if placed in operational areas, report directly to the head of the service for matters pertaining to their tasks.

Annex 1 (Internal Information Flows) details the cases in which the Group Anti-Money Laundering Service reports to the Corporate Bodies directly or through the person responsible for anti-money laundering. In any case, the Group Anti-Money Laundering Service may report directly in the event of significant violations and deficiencies.

2.8. Head of Group Anti-Money Laundering Service

The head of the Group Anti-Money Laundering Service is appointed by the Board of Directors - after consulting the Board of Statutory Auditors, on the proposal of the Control and Risk Committee and with the input of the Appointments Committee.

The same must, also pursuant to Article 20 of Ministry of Economy and Finance Decree No. 169 of 23 November 2020:

1) possess adequate requirements of independence, competence, professionalism and reputation, honesty and integrity;
2) must be provided with adequate time and resources in order to perform its tasks effectively;
3) must have sufficient decision-making power to be able to operate effectively for ML/TF risk management and prevention purposes, in accordance with the principle of proportionality and the applicable legislation;
4) must possess adequate knowledge, skills and experience regarding money laundering risks, AML/CTF policies, controls and procedures, and the Group-wide *business* model.

He is one of the heads of corporate control functions, and is therefore placed in an appropriate hierarchical-functional position, does not have direct responsibility for operational structures and is not hierarchically subordinate to persons responsible for such areas. He reports to the Corporate Bodies of the Parent Company, either directly or through the representative responsible for anti-money laundering, in accordance with Appendix 1, and reports hierarchically to the Managing Director.

In the event of absence or impediment, the duties of the head of the Group Anti-Money Laundering Service are performed by a delegate, appointed by the Board of Directors of the Parent Company, as provided for in paragraph 2.1. The delegate appointed must have the appropriate skills and experience to assume the functions of the manager in the cases set out above.

At least twice a year, the Head of the Group Anti-Money Laundering Service draws up and transmits - directly or through the person responsible for anti-money laundering in accordance with Appendix 1 - to the Board of Directors, the Managing Director and the Board of Statutory Auditors a report, also at Group level, on the initiatives taken, the anomalies ascertained and the relevant corrective action to be taken, as well as on staff training activities. The report also includes the results of the Group self-assessment exercise, in accordance with the procedures indicated in paragraph 5.

The report of the Group Anti-Money Laundering Officer must include at least the following points, based on data provided by the AML officers of the individual banking group companies:

a. consolidated statistics at Group level concerning, in particular, risk exposure and suspicious transaction reports;
b. monitoring of inherent risks that have occurred in one or more Group companies and an analysis of the impact of residual risks;
c. supervisory reviews, internal or external audits, including serious deficiencies identified in the Group's AML/CFT policies and procedures, as well as actions or recommendations for corrective measures;
d. information on the supervision and supervision of subsidiaries and branches located in high-risk countries, if any.

As regards information flows to and from the individual AML structures of the individual Group members and to and from the corporate bodies, these are detailed in Appendices 1 and 2 ("Internal Information Flows" and "Intra-Group Information Flows").

The bank transmits to the Bank of Italy, within twenty days of the relevant resolution, the decision to appoint or revoke the Group Anti-Money Laundering Officer.

2.9. Office AML of BPS

The AML office of BPS (Banca Popolare di Sondrio) falls within the second level of the internal control system, reports through the head of the Group Anti-Money Laundering Service to the Bodies with strategic supervision, management and control functions and has access to all the bank's activities, as well as to any information relevant to the performance of its tasks.

The office is qualitatively and quantitatively well resourced for the tasks to be performed.

The personnel performing tasks attributable to the AML office of BPS are adequate in number, technical-professional skills and up-to-date, including through ongoing training programmes.

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

- identifies the applicable standards and assesses their impact on internal processes and procedures;
- collaborates in defining the system of internal controls and procedures aimed at preventing and combating money laundering risks;
- continuously verifies the adequacy of the risk management process and the suitability of the system of internal controls and procedures and proposes organisational and procedural changes to ensure adequate risk management;
- conducts, through its manager, in liaison with the other corporate functions concerned, the annual self-assessment exercise of the money laundering risks to which the bank is exposed, in accordance with paragraph 5, to be forwarded to the Group Anti-Money Laundering Officer;

- submits to the Board of Directors on an annual basis, through the service manager, a plan of activities, including both the second-level checks to be carried out and any organisational and/or technical/IT measures required to strengthen the controls in the area of customer due diligence, the reporting of suspicious transactions and the retention of data, information and documents;
- recommends to the body with management function the corrective measures to be taken to remedy any weaknesses detected, including by the competent authority and the Internal Audit;
- conducts checks on the functionality of the reporting process and the appropriateness of the assessments made by the first level on customer transactions;
- collaborates in the definition of policies to govern money laundering risk and the various stages in the process of managing that risk;
- provides support and assistance to corporate bodies and senior management;
- assesses on a preventive basis the money laundering risk associated with offering new products and services, significantly altering products or services already offered, entering a new market or starting new activities, and recommends the measures necessary to mitigate and manage the possible risks;
- verifies the reliability of the information system for the fulfilment of customer due diligence obligations, for the storage and provision of documents, data and information, and for the reporting of suspicious transactions;
- transmits monthly aggregated data to the FIU concerning its overall operations, in accordance with the 'Provisions for sending aggregated data' published by the FIU on 25 August 2020;
- transmits to the FIU, on the basis of instructions issued by it, objective communications concerning transactions at risk of money laundering;
- defines, in agreement with the reporting officer, procedures for handling internal reports (from the so-called 'first level') concerning particularly high-risk situations to be treated with due urgency;
- ensures, in cooperation with the relevant corporate functions, the preparation of an adequate training plan, aimed at achieving continuous updating of employees and collaborators and of indicators of the effectiveness of the training activities carried out;
- promptly informs, through the head of the service, the corporate bodies of significant violations or deficiencies encountered in the performance of their duties;
- periodically informs the corporate bodies - either directly or through the person responsible for anti-money laundering in accordance with the provisions of Appendix 1 - on the progress of the corrective actions taken in the face of deficiencies found in the control activity and on the possible inadequacy of the human and technical resources assigned to the anti-money laundering function and the need to strengthen them;
- prepares direct information flows to the corporate bodies, the anti-money laundering officer

and top management;

- performs enhanced customer due diligence in relation to particular circumstances - objective, environmental or subjective - in which the risk of money laundering is particularly high;
- makes notifications of infringements pursuant to Article 49 of Legislative Decree 231/2007 to the Ministry of Economy and Finance.

The AML department of BPS draws up a document which defines in detail the responsibilities, tasks and operating procedures in the management of the money laundering risk (so-called 'AML manual'). After being validated by the Group AML Officer, it is forwarded by the latter to the Managing Director and the Board of Directors.

In assessing the adequacy of internal procedures for preventing and combating money laundering risk, the BPS AML Office, also in liaison with the Internal Audit Service, may carry out on-site checks to verify their effectiveness and functionality.

Further details on the attributions of the BPS AML Office can be found in the 'Regulation of the BPS AML Office'.

2.10. Office Manager AML of BPS

The head of BPS's AML office is appointed by the Managing Director and meets the appropriate requirements of independence, authority and professionalism.

Prior to appointment, it must be verified that he/she is in possession of:

a) an adequate reputational profile, honesty and integrity necessary to perform their function;
b) appropriate skills and experience in AML/CFT, including knowledge of the applicable legal framework and in the implementation of policies, controls and procedures in this area and in the identification, assessment and management of ML/FT risks;
c) sufficient knowledge and understanding of the ML/FT risks associated with the bank's *business* model to enable it to perform its function effectively;
d) adequate experience in the identification and management of ML/TF risks;
e) adequate time and hierarchical position to perform their duties effectively, independently and autonomously.

If he/she is entrusted with other tasks, the head of the service must assess potential conflicts of interest and propose specific measures to prevent or manage them to the Deputy Director. Moreover, in the presence of other assignments, the head of the AML office must be able to devote sufficient time to the performance of his duties.

The head of the BPS AML office:

- for the purpose of identifying and considering risks, supports the Head of Service in the development of a ML/TF risk assessment framework for analysis at the individual relationship

and business area level, in line with Bank of Italy and EBA Risk Factor Guidelines;

- supports the service manager in the development of AML/CTF policies and procedures to be implemented by the bank and keeps them up-to-date, including in relation to changes in laws or regulations;
- communicates, directly or through the person responsible for anti-money laundering in accordance with Annex 1, the results of the risk assessment on an individual or business area basis to the Board of Directors;
- assesses ML/FT risks related to the introduction of new products or services or major changes to existing products or services, the development of a new market or the start-up of new activities;
- proposes ways to address any changes in legal or regulatory requirements or ML/CTF risks that are necessary to address any gaps or deficiencies identified through the audit activity;
- must be consulted by senior management prior to the decision to accept new high-risk customers or on the continuation of such relationships, especially in cases where senior management approval is expressly required pursuant to Directive (EU) 2015/849 and the Anti-Money Laundering Decree;
- supervises the effective implementation of controls by *business* lines and internal units (so-called first level);
- submit - directly or through the person responsible for anti-money laundering - to the Board of Directors the corrective measures to be taken to remedy weaknesses, including those identified by the competent authorities, external auditors and the Internal Audit function;
- periodically informs - directly or through the person in charge of AML - the Managing Director of the progress of the measures adopted or recommended and, where appropriate, of the possible inadequacy of the human and technical resources assigned to the AML office of BPS and of the consequent need to strengthen them.

The head of the AML office of BPS may entrust and delegate his tasks to other employees working under his direction and supervision, but he remains ultimately responsible for the actual performance of those tasks.

If the head of the BPS AML office works for two or more Group entities and/or is entrusted with other functions, he/she must be put in a position to effectively perform his/her duties.

2.11. Group AML Office

The Group AML office reports hierarchically to the head of the Group AML department and is endowed with qualitatively and quantitatively adequate resources for the tasks to be performed.

The heads of the AML department, or similar structures, of each subsidiary may communicate directly with the head of the Group AML department.

The Group AML office:

- constitutes a coordinating unit for all Group companies, so that they implement Group

policy and adopt adequate and appropriate systems and procedures for the effective prevention of ML/TF, consistent with the structure of the Group and the size and characteristics of each intermediary;

- sets up internal control mechanisms on AML/CFT at Group level;
- cooperates, through its manager, with the anti-money laundering functions or similar structures of each Group entity.

With regard to information flows to and from the individual anti-money laundering functions of the individual Group components and to and from the corporate bodies, these are detailed in Appendices 1 and 2 ("Internal Information Flows" and "Intra-Group Information Flows").

2.12. Group AML Office Manager

The Head of the Group AML Office is appointed by the Group AML Officer, subject to the endorsement of the Managing Director, and possesses appropriate requirements of independence, authority and professionalism.

Prior to appointment, it must be verified that he/she is in possession of:

a)an adequate reputational profile, honesty and integrity necessary to perform one's function;

(b) appropriate AML/CFT skills and experience, including knowledge of the applicable legal framework and in the implementation of AML/CFT policies, controls and procedures and in the identification, assessment and management of ML/FT risks;

c) sufficient knowledge and understanding of the ML/FT risks associated with the Group's *business* model to enable it to perform its function effectively;

d) adequate experience in the identification and management of ML/TF risks;

e) adequate time and hierarchical position to perform their duties effectively, independently and autonomously.

If he/she is entrusted with other tasks, the head of the department must assess potential conflicts of interest and propose specific measures to the Managing Director to prevent or manage them. Moreover, in the presence of other assignments, the head of the Group AML office must be able to devote sufficient time to the performance of his duties.

The head of the Group AML office:

- oversees the money laundering risk assessment exercise conducted by the Group's components;
- cooperates fully with the Anti-Money Laundering Officer of each Group entity;
- coordinates the *business* area-wide assessment of ML/TF risks at the local level by the various Group companies and organises the aggregation of their findings, in order to understand the nature, intensity and location of ML/TF risks to which the Group as a whole is exposed;
- coordinates the activities of the various AML officers of Group entities to ensure that they

operate consistently;

- draws up and submits to the Parent Company's bodies anti-money laundering procedures, methodologies and group standards and ensures that the policies and procedures of the group's components are in line with these *standards*, as well as with the relevant laws and regulations applicable to them;
- establishes regular information flows from all Group companies to share the information necessary to perform their tasks;
- monitors the compliance of subsidiaries and branches located in non-EU countries with EU AML/CFT requirements, in particular where the requirements for the prevention of ML/TF are less stringent than those of Directive (EU) 2015/849.

2.13. Head of suspicious transaction reports of Banca Popolare di Sondrio

Pursuant to Article 36 of the Anti-Money Laundering Decree, the person responsible for reporting suspicious transactions (or STR) is the legal representative of the recipient or a proxy of the recipient; the proxy may also be conferred on the head of the Group Anti-Money Laundering Service. The delegation of authority is decided by the Board of Directors, after consulting the Board of Statutory Auditors.

The person in charge of the STR has adequate requirements of independence, authority and professionalism and carries out his or her activity with autonomy of judgement and in compliance with the confidentiality obligations provided for by the anti-money laundering decree, also with regard to the representatives and other corporate functions. The role of the STR manager is suitably formalised and made known within the structure and to the territorial network. The appointment and revocation of the same officer is promptly communicated to the FIU in the manner indicated by it.

The STR manager has no direct responsibilities in operational areas and is not hierarchically subordinate to persons belonging to those areas. He must verify that any human resources entrusted with the task of analysing computerised transactions and *alerts have the* necessary skills, knowledge and suitability and are adequately informed of the bank's obligations to keep information confidential and protect the reporter.

The STR manager is familiar with the structure and selection criteria of the operation monitoring systems and the internal procedures for handling *alerts* and periodically verifies their proper functioning.

He may receive reports from employees of the network, business units and offices, or from the bank's bodies, ensuring that they are assessed in a timely manner. To this end, the STR manager defines a process for prioritising the internal reports received, in proportion to their risk.

The person responsible for reporting suspicious transactions:

- promptly assesses, in the light of all available elements, suspicious transactions reported by the head of the branch or other operational point or organisational unit or structure responsible for the concrete management of customer relations (so-called first level);

- promptly assess, in the light of all available elements, suspicious transactions of which it has otherwise become aware in the course of its activities;
- transmits to the FIU the reports it considers well-founded, omitting the names of the persons involved in the transaction reporting procedure;
- keeps evidence of the assessments made under the procedure, even if the report is not sent to the FIU, in compliance with confidentiality obligations;
- acquires any useful information from the structure carrying out the first level of analysis of anomalous transactions and from the Group Anti-Money Laundering Service;
- has free access to information flows directed to corporate bodies and structures and/or functions that are significant for preventing and combating money laundering and terrorist financing (e.g. requests received from judicial authorities or investigative bodies);
- assessments also use information on any STR already carried out on the same customer by other Italian group companies;
- It also considers any additional elements that can be deduced from freely accessible information sources (e.g. search engines, journalistic sources, etc.);
- plays a liaison role with the FIU and investigative bodies and responds promptly to any requests for further information from them.

The STR manager communicates, in an organisational manner that ensures compliance with the confidentiality obligations laid down in the Anti-Money Laundering Decree, the outcome of his assessment to the first-tier responsible person who originated the report.

In compliance with the confidentiality obligations provided for by the anti-money laundering decree on the identity of the persons taking part in the transaction reporting procedure, the STR manager provides - also through the use of appropriate information bases - information on the names of the customers subject to suspicious transaction reports to the heads of the structures responsible for assigning or updating the risk profile of such customers.

Further guidance on the role of the suspicious transaction reporter and the reporting process is detailed in the bank's 'Rules for reporting suspicious transactions'.

2.14. Risk Control Service

With regard to the control of money laundering and terrorist financing risks, the Risk Control Department cooperates with the Group Anti-Money Laundering Department and its manager:

- for the definition of AML/CFT risk assessment methodologies, fostering synergies with *operational risk management* tools and methods;
- to integrate the non-compliance risk assessment and management model into the *Risk Appetite Framework*;
- in the analysis of risks associated with new products and services to be marketed, including with regard to entry into new activities and new markets, both on request and through a structured *clearing* process, collaborating in the identification of potential risks for the bank and customers and providing quantitative assessments where applicable.

2.15. Operational Structures

The company's operational structures represent the first and essential level of corporate supervision for the purposes of preventing and combating money laundering and terrorist financing phenomena, inasmuch as they are the operating units concretely responsible for the administration and management of customer relations. In particular:

- transpose the operational instructions on anti-money laundering and anti-terrorism, provided for by external and internal regulations;
- carry out their customer due diligence obligations, both at the stage of establishing ongoing relations and on occasional customers, also carrying out constant monitoring throughout the duration of the relations, including through the use of IT tools specifically intended for that purpose;
- acquire and ensure the orderly storage of the documents, data and information required for the fulfilment of customer due diligence obligations, in accordance with internal rules, and ensure that they are kept up-to-date;
- on the basis of the evidence provided through the specifically designated instruments, carry out periodic assessments of the risk profile attributed to customers;
- assess the transactions carried out by customers, including - but not exclusively - through the supporting IT tools set up for this purpose, activating, where appropriate, the suspicious transaction reporting process;
- review the periodic evidence provided from time to time by the competent central services or offices to ensure compliance with the customer due diligence requirements;
- ensure the utmost cooperation with the competent Authorities, within the framework of investigations, in-depth investigations, inspections on money laundering and terrorist financing carried out at their premises, coordinating with the competent structures and/or functions of the company.

2.16. Branch Anti-Money Laundering Contacts

At each branch of the bank, a branch contact person is identified - by the head of the branch - who is specially trained in the subject matter, and who, while reporting hierarchically to the head of the branch, coordinates, where necessary, with the AML office of BPS in order to

- be the interlocutor within the branch towards the AML office of BPS, both for requests for advice from the branch and for requests received from the central service;
- ensuring the circulation of information within the operational structure, avoiding redundancy in requests for information or assistance, receiving and responding to queries within the dependency and involving the BPS AML office if support is needed;
- support the Head of Dependency in the ongoing assessment of customer operations and the detection of any suspicious transactions.

The branch anti-money laundering contact person does not, as such, assume the responsibilities attributed by law to the head of the branch.

3. MONEY LAUNDERING AND TERRORIST FINANCING RISK MANAGEMENT MODEL OF THE BANKING GROUP

The Banca Popolare di Sondrio Banking Group adopts a unified approach to anti-money laundering and combating the financing of terrorism, with guidelines, rules, processes, controls and IT tools that are as homogeneous as possible. To this end, the companies of the Banking Group are required to transpose this Document, adapting it to their own corporate context and, in the case of foreign subsidiaries, to the specificities of local regulations, submitting it to the approval of the Body with strategic supervisory functions. The Banking Group's subsidiaries shall inform the bank of the outcome of the transposition process in accordance with the procedures set forth in the "Corporate Rules and Regulations" of 30 June 2023.

Strategic decisions at the Banking Group level on AML/CFT risk management and related controls are left to the Corporate Bodies of the Parent Company. The latter ensures that the Corporate Bodies of the other Group companies implement the Group's AML/CFT strategies and policies in their own companies and ensures that the Bodies and internal structures of each component, including their respective control functions, have the necessary information to perform their duties.

The Parent Company appoints a member of the Board of Directors to be responsible for anti-money laundering at Group level. The appointment is of an executive nature. The Group Anti-Money Laundering Officer is the main point of contact between the Group Anti-Money Laundering Officer and the Bodies with strategic oversight and management functions of the Parent Company, and ensures that the latter have the necessary information to fully understand the significance of the money laundering risks to which the Group is exposed, for the purpose of exercising their respective powers. The Group Anti-Money Laundering Officer ensures that the Group Anti-Money Laundering Officer performs his or her duties effectively.

The representative responsible for money laundering at Group level may be the same as the representative responsible for the parent company.

The Corporate Bodies of the Banking Group's subsidiaries must be aware of the choices made by the Corporate Bodies of the Parent Company and are responsible, each according to his or her competencies, for the implementation of money laundering and terrorist financing risk management strategies and policies in line with his or her own corporate reality. With this in mind, the Parent Company involves and informs, through the Managing Director and the Head of the Group Anti-Money Laundering Service, the Corporate Bodies of the investee companies on the choices made regarding policies, processes and procedures for managing the risk of money laundering and terrorist financing.

The Parent Company defines and approves at banking group level:

- a Group methodology for assessing the risk of money laundering and terrorist financing;
- general *standards on* due diligence requirements, the retention and making available of documents, data and information, and the detection and reporting of suspicious transactions;

- formalised procedures for the coordination and sharing of relevant information on the subject within the Banking Group, including for the purpose of identifying suspicious transactions, and a direct reporting line between the heads of the anti-money laundering functions of the components, including foreign components (compatible with the legal regimes of third countries), of the Group and the Group Anti-Money Laundering Officer;
- Group-wide anti-money laundering control procedures.

The parent company identifies suitable organisational solutions to ensure compliance with the applicable provisions in relation to the various areas of operations, periodically assesses the effectiveness and functionality of the Group's anti-money laundering policies and procedures, and ensures that the management of money laundering risks takes into account all the evaluation and measurement elements in its possession.

The Parent Company ensures that Group entities promptly implement the necessary corrective measures to overcome deficiencies in anti-money laundering controls identified by the Bank of Italy, the FIU or, in relation to foreign components, the competent authorities.

Within the Banking Group, the specific tasks assigned to the Group Anti-Money Laundering Service are carried out on the basis of two distinct models, declined to take account of the operational and territorial articulation of the Banking Group itself. In particular:

1) In the case of Banca della Nuova Terra Spa, whose operations are characterised by a high level of integration with the Parent Company, it is planned to *outsource* AML/CFT risk control activities to the Group's AML department, with the simultaneous appointment of an internal contact person (RAE) at the subsidiary;
2) For Banca Popolare di Sondrio Spa, Factorit Spa and Banca Popolare di Sondrio (SUISSE), the establishment of autonomous anti-money laundering structures and the appointment of a person responsible for each of them is established.

In the first case, the AML and terrorist financing risk control activities are carried out by the BPS AML office and the related activities performed are governed by specific outsourcing contracts. In addition, an internal anti-money laundering contact person (RAE) is appointed who, operating in close functional coordination with the Group AML office, oversees the processes related to AML/CFT regulations within the individual subsidiary.

The outsourced anti-money laundering structure - on the basis of the guiding principles and *standards of* conduct established by the Group Anti-Money Laundering Service, which Banca della Nuova Terra must follow for the management of the main obligations in question -

- identifies and updates the system of first- and second-level controls;
- defines the requirements of the tools supporting the processes of customer due diligence and profiling and intervenes in the assessment process of customers with a high risk profile;
- supervises the storage of information, documents and data for the fulfilment of anti-money laundering obligations;
- prepares periodic summary reports, or specific *reports* in the case of particularly serious events, to be forwarded to the corporate bodies and top management.

The internal contact person appointed at the subsidiary has the task of verifying the proper performance of the service by the outsourced anti-money laundering structure and adopts the organisational precautions necessary to ensure the maintenance of the powers of direction and control by the corporate bodies. In particular:

- monitors, through periodic checks, compliance with contractual obligations and the proper performance of the service by the outsourced function;
- verifies that the service provided enables the effective fulfilment of anti-money laundering obligations;
- regularly reports to the corporate bodies on the performance of the outsourced tasks, so as to ensure that any necessary corrective measures are promptly taken.

For the subsidiaries of the Banking Group to which the second model applies - Factorit Spa and Banca Popolare di Sondrio (SUISSE) -, on the other hand, an autonomous anti-money laundering structure is set up and the relevant person in charge is appointed (who may also be delegated to report suspicious transactions):

- operates in coordination with the head of the Group AML office and informs him/her of the results of the control activities carried out and of any significant events;
- ensures that the head of the Group AML office, subject to applicable national regulations, has access to all data and information necessary to assess ML/FT risks;
- liaises with the competent supervisory authorities, coordinating with the Group AML office.

With regard to the reporting of suspicious transactions, the organisational model at the Banking Group level provides for the appointment, by the Board of Directors of each subsidiary subject to the relevant regulatory obligations, having consulted the Board of Statutory Auditors, of a corporate STR manager for the reporting of suspicious transactions. In order to ensure the existence of appropriate coordination mechanisms to safeguard the homogeneity and consistency of the analysis logics employed, the STR manager appointed at the Parent Company, for the purposes of investigating anomalous transactions and relations within the Banking Group, interfaces with the STR managers at the subsidiaries, in order to share data and information relating to common customers in respect of whom a reporting *process* has been commenced, without prejudice to the regulatory limits in foreign jurisdictions, as better described in paragraph 3.1. In any case, the confidentiality of the identity of the persons participating in the reporting procedure is guaranteed.

In general, the Group AML office has access to all activities and any information relevant to the performance of its tasks.

The head of the Group's AML office has an information base that allows a homogeneous assessment of the customers shared by the Group's Italian companies. With regard to the Swiss subsidiary, due to the restrictions on the exchange of information that remain in Swiss law, the data subject to sharing relates to BPS (SUISSE) customers reported for suspicious transactions and those considered high risk, as better explained in paragraph 3.1.

In particular, the following information is shared among all companies based in Italy:

- master data of common customers;
- risk profiles of common customers;
- reports of suspicious transactions made against ordinary customers, together with the reasons for them.

The Board of Directors of the Parent Company verifies:

- that each Group company assesses its respective money laundering and terrorist financing risks in a coordinated manner and on the basis of the parent company guidelines, while taking into account their respective specificities;
- that, in the event of supervisory activities carried out on a Group company, the corrective measures taken by that company to remedy any deficiencies found are implemented in a timely and effective manner.

3.1. ML/FT risk management in relation to the foreign subsidiary Banca Popolare di Sondrio (SUISSE)

Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for minimum action and the type of additional measures to be taken by credit and financial institutions to mitigate the risk of money laundering and terrorist financing in certain third countries, provides for additional measures - including minimum action - to be taken by credit and financial institutions to effectively address the risks in question in cases where the legal system of a third country does not allow the implementation of group policies and procedures as referred to in Article 45(1) and (3) of Directive (EU) 2015/849 (c.d. Fourth Anti-Money Laundering Directive), at the level of branches or majority-owned subsidiaries which are part of the Group and which are established in a third country.

In addition, where the legal system of the third country prohibits or limits the implementation of policies and procedures necessary to appropriately identify and assess the money laundering and terrorist financing risk associated with a business relationship or occasional transaction, by restricting access to relevant customer and beneficial ownership information, or by limiting the sharing and use of such information for customer due diligence purposes credit and financial institutions must, inter alia, at a minimum "*disclose to the competent supervisory authority of the home Member State without delay how the application of the third country's legislation prohibits or restricts the implementation of policies and procedures necessary to identify and assess money laundering and financing risk associated with a customer*". In concrete terms, as also provided for in the Bank of Italy's Provision "Provisions on organisation, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing" of 26 March 2019, "*The Parent Company shall establish a common information base that allows all companies belonging to the group to assess customers in a homogeneous manner*". In the event of impossibility, "*The Parent Company shall notify the Bank of Italy within the terms and in the manner provided for in the European Commission regulation pursuant to Article 45(7) of the AML Directive and shall take further measures indicated therein*".

As highlighted to the Bank of Italy by the Parent Company of the Banca Popolare di Sondrio Banking Group, in a specific communication, the contents of which were approved at the Board meeting of 20 December 2019, the Swiss regulatory provisions on constraints and restrictions limit the possibility of sharing and processing, within the Group, data on the subsidiary's customers and their risk profile, as well as information on suspicious transaction reports. Similar restrictions apply to the local regulations in force at the branch of Banca Popolare di Sondrio SUISSE located in the Principality of Monaco.

Subsequently, on 26 June 2020 - in response to the Bank of Italy communication of 19 April 2020 concerning Banca Popolare di Sondrio. Communication pursuant to Delegated Regulation (EU) 2019/758: request for clarification - the Board of Directors of the Parent Company, on 20 June 2020, provided that - in addition to the indicators and data flows and information of an aggregate nature that the Swiss subsidiary already provides - "*upon the detection of situations with a high risk of money laundering and terrorist financing, likely to create legal and reputational issues at Group level, the subsidiary shall make available to the Parent Company's control functions the information available at the Parent Company, including information concerning certain business relationships. The assessment of individual cases and the coordination of the provision of the above-mentioned information are ensured, as a rule - except in cases of urgency - by bimonthly discussions between the head of the subsidiary's Legal & Compliance department and the head of the Group Anti-Money Laundering department at the subsidiary*'.

In light of the above, below are the methods and procedures through which the Parent Company implements the control of money laundering and terrorist financing risks in respect of its subsidiary Banca Popolare di Sondrio (SUISSE) SA, including the branch in the Principality of Monaco, as defined by the Board of Directors.

In this regard, it should be noted that a *Compliance officer is* appointed at the Monaco branch, responsible for anti-money laundering, who reports functionally to the head of the *Legal & Compliance* department of the Swiss parent company.

Specifically, through:

a. the provision - by the subsidiary - of aggregated information flows;
b. the preparation - by the subsidiary - of periodic reports;
c. bi-monthly coordination and sharing meetings at BPS (SUISSE) between the heads of the 'AML' structures;
d. interactions between the head of the BPS *Legal & Compliance department* (SUISSE) and the head of the Group Anti-Money Laundering department for matters of an urgent nature or upon the occurrence of events exceeding certain attention thresholds;
e. submission by the Parent Company of the so-called Country List.

a. Aggregate information flows

BPS (SUISSE), on a monthly basis, sends a set of indicators to the parent company, described below.

INDICATOR	CONTENT
Customer distribution by risk bracket[4]	The stream provided reports to the end date of the reporting period: - the distribution of customers, divided between natural persons and legal entities; - distribution of reports per risk band; - manual changes in the risk band (decreases/increases); - distribution of subjects by risk factors; - distribution of relationships with risk factors, with evidence of how many opened during the reporting period; - number of incomplete/missing due diligence information; - number of events for updating the due diligence.
Operations with countries at risk[5]	The stream provided reports to the end date of the reporting period: - distribution of subjects by country risk with country evidence and subsequent breakdown; - Distribution of fund transfers by country risk with country evidence in terms of amounts and number of transactions.
Distribution and matching situations of names to those on external lists	The flow provided includes: - number of reports highlighted to the *Legal & Compliance* department on opening by the IT solution (CREA)[6] , for verification of possible correspondence; - number of reports, at the opening stage, matching names actually ascertained; - number of matches found in the *AML-Bestvision* procedure[7] during the reporting period; - number of relationships in place at the end of the reporting period; - number of concordances in AML procedure confirmed during the reporting period; - number of transactions 'put on hold' by the *Fircosoft* procedure[8] ; - number of transactions verified by the *Fircosoft* application during the reporting period; - types of subjects confirmed.
Indicators of abnormal or unexpected behaviour (so-called 'plausibilisation')	The stream provided reports to the end date of the reporting period: - distribution of the unexpected by type of behaviour; - distribution of the unexpected by evaluation time; - distribution of unexpected non-assessments, both from Level I and Level II.
Distribution of suspicious transaction	The flow provided shows the number of suspicious transaction reports sent to the

[4] At BPS (SUISSE), the categorisation of customer risk profiles is different from that of the parent company. Specifically: Level A (PEP); Level B (policyholder and/or procurer and/or beneficial owner with domicile and profession at risk); Level C (domicile of the policyholder and/or procurer and/or beneficial owner in a country at risk); Level C1 (domicile of the control holder in a country at risk) Level C2 (place of business of the contracting party and/or beneficial owner in a high-risk or non-cooperative country according to the FATF); Level C3 (regular relationship (belonging to Band E) that, on a half-yearly basis, for a volume of 25% or more, totalling more than 30.000 CHF, receives or sends from or to high-risk or non-cooperative countries according to the FATF); Level D (profession/business activity at risk of the owner and/or attorney and/or beneficial owner); Level D1 (relationships with assets in excess of 5 million CHF; Level E (all other relationships not covered by the higher risk categories); Level F (relationships requiring special monitoring); Level G (complex structures).

[5] The definition of 'risk countries' for Swiss legislation is partially different from that of the parent company: 'sanctioned' countries are those decreed by the UN, the EU and the State Secretariat for Economic Affairs (SECO).

[6] *CREA*, an IT solution expressly dedicated to the automatic verification, through direct interfacing with the *WorldCheck* and *Compliance Daily Control* lists, of the names *of* potential customers and other possible participants in the relationship.

[7] *AML-Bestvision*, an IT solution dedicated to assessing 'higher risk' transactions and monitoring tax compliance.

[8] *Fircosoft/Stelink*, IT solution for monitoring transactions with payer and/or payee included in the *WorldCheck* lists.

reports (STR)	Money Laundering Reporting Office (MROS) at the end of the reporting period, with a distribution: - by category; - by type; - by origin; - by number of secondary subjects involved; - by number of operations; - by amount band; - by forwarding time (with evidence of the average value); - by type of storage.

b. Periodic reports

INFORMATION FLOW	SENDER	DESTINATORY	FREQUENCY
Report on the *compliance* risk assessment and activities carried out by the *Legal & Compliance* department	subsidiary's *Legal & Compliance* department	- Compliance function of BPS - Group Anti-Money Laundering Service	Half-yearly (data as at 30 June) and annual (data as at 31 December), subject to approval by the subsidiary's Board of Directors
Action plan with measures to be prepared during the year	subsidiary's *Legal & Compliance* department	- Compliance function of BPS - Group Anti-Money Laundering Service	Annual, subject to approval by the Board of Directors of the subsidiary
Update of the action plan and progress of activities	subsidiary's *Legal & Compliance* department	- Compliance function of BPS - Group Anti-Money Laundering Service	Annual, subject to approval by the Board of Directors of the subsidiary

c. Bi-monthly coordination meetings

With a view to proactively combating money laundering and terrorist financing, specific meetings are held on a bimonthly basis_- except in cases of urgency, for situations considered high risk, requiring immediate sharing with the parent company - between the head of the *Legal & Compliance* office of the BPS (SUISSE), the Group Anti-Money Laundering manager and the head of the Group AML office. During these meetings, which are usually held at the head office in Lugano, the personal data of names subject to suspicious transaction reports sent to the competent Authorities by the Swiss parent company and the Munich branch are, among other things, shared. In addition, the parent company provided a list containing the names of persons reported by it for suspicious transactions in the two months preceding the meeting. At the next meeting, the subsidiary will provide evidence of the existence of common customers with those subject to STR by the Parent Company, indicating, where appropriate, the measures taken to mitigate any risk situations. The Group's Anti-Money Laundering Service will verify all the names on the list provided by the subsidiary; in the event of any matches, the service itself will carry out the necessary checks and investigations in order to manage any emerging money laundering and terrorist financing risks. On a continuous monthly basis, the Group Anti-Money Laundering

Service will renew the above-mentioned checks on the entire list of names communicated from time to time and subject to reporting for suspicious or higher risk transactions.

d. Further coordination meetings and attention thresholds ('*triggers*')

In the event that the head of the *Legal & Compliance department* and/or the head of the Group Anti-Money Laundering department should find it necessary to align on certain issues that could have a negative impact on the risk of money laundering and terrorist financing - or even only from a reputational point of view - they will take steps, even in the shortest possible time, to ensure that the necessary steps are taken, if deemed necessary also through specific meetings at the Lugano branch of the subsidiary.

In the event of absence or impossibility, the Group Anti-Money Laundering Officer may make direct contact with the contact person of the BPS (SUISSE) Compliance Office and, as a last resort, with the Chairman of the Executive Board.

The events and related attention thresholds ('*triggers*'), upon the occurrence of which the Group Anti-Money Laundering Service must carry out additional checks and investigations against the subsidiary, are as follows:

TRIGGER	THRESHOLD	ADDITIONAL MEASURES
PEP customers as a percentage of total customers	≥ 0,15%	Request to the local *Legal & Compliance* department of BPS (SUISSE) to provide clarification in writing as to the reasons why the threshold was exceeded, the type of customers concerned and the corresponding ML/TF risk mitigation measures taken
Incidence of customers classified as high risk out of total customers	≥ 3%	Request to the local *Legal & Compliance* department of BPS (SUISSE) to provide clarification in writing as to the reasons why the threshold was exceeded, the type of customers concerned and the corresponding ML/TF risk mitigation measures taken
Incidence of no. of transactions to countries subject to EDD; Incidence of the amount of transactions to EDD countries	≥ 0,60% ≥ 1,30%	Request to the local *Legal & Compliance* department of BPS (SUISSE) to provide clarification in writing as to the reasons why the threshold was exceeded, the type of customers concerned and the corresponding ML/TF risk mitigation measures taken
Presence of findings by the external auditor or the local supervisory authority	a event	Constant monitoring of the consequent actions, in compliance with the deadlines set for adaptation

If the Head of the Group Anti-Money Laundering Department sees the need for further investigation, he may request further information from the *Legal & Compliance* Department of BPS (SUISSE) - possibly also on site - involving, where deemed appropriate, also the Corporate Bodies of the subsidiary and, in the most serious cases, also the Board of Directors of the Parent Company and the representative responsible for anti-money laundering of BPS and the Group.

During on-site visits, the Group Anti-Money Laundering Officer must also request information and documentation relating to suspicious transaction reports forwarded by the subsidiary to the local (Swiss and/or Monegasque) authority.

e. Transmission Country Table

The Group's AML Office provides all the Banking Group's subsidiaries, including BPS (SUISSE), with the Country Table drawn up in accordance with the criteria illustrated in paragraph 4.2, on the occasion of each update. As far as the Group's Italian companies are concerned, the risk profile assigned to each country is relevant (together with other factors) for the purposes of assigning the risk profile to individual customers, as well as in the context of the depth and extent of the due diligence measures applicable to individual transactions from/to third countries.

With regard to the subsidiary BPS (SUISSE), the Country Table is used to provide the Parent Company with consistent data on transactions from/to non-EU countries (other than Switzerland and the Principality of Monaco), as part of the preparation of monthly and quarterly risk indicators. In addition, it is used in the AML/CFT risk self-assessment performed twice a year (on 30 June and 31 December) and reported to the Parent Company for the Group's self-assessment.

4. EXPOSURE TO AND MANAGEMENT OF AML/CTF AND INTERNATIONAL FINANCIAL EMBARGOES AND SANCTIONS RISKS

Banca Popolare di Sondrio proposes itself on the market as a universal bank, combining its tradition as a company strongly rooted in the territory with its great attention to the development of international relations.

Given the nature, size and complexity of its business and the type and range of services provided, the bank is exposed to money laundering and terrorist financing risk, which is monitored by the Group Anti-Money Laundering Service, including through the self-assessment exercise, in order to maintain an organisational structure, operating and control procedures and information systems that are suitable for ensuring compliance with legal and regulatory provisions on countering the aforementioned risks.

For details on the self-assessment exercise, please refer to the specific paragraph 5 of this Document ("AML/CFT risk self-assessment and annual report"). The BPS AML Office - through this periodic exercise - identifies the current and potential risks to which the bank is exposed ("inherent risk") and the level of adequacy of its organisational set-up ("vulnerability analysis").

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

Based on the level of residual risk determined, and taking into account the vulnerability analysis, the bank identifies the corrective or remedial action to be taken to prevent and mitigate the residual risks. These measures are implemented by the Management Body through the Group Anti-Money Laundering Department, which is also responsible for monitoring the progress of the planned adaptation measures.

In this context, BPS's AML office updates the results of the last self-assessment exercise conducted every six months, adjusting the vulnerability analysis in the light of the implementation of the planned adaptation measures.

In determining the vulnerability analysis, the bank assesses the organisational set-up, operational and control procedures, and information systems adopted to ensure compliance with the statutory and regulatory requirements in the area of anti-money laundering. In making this assessment, the bank also takes into account the indications and evaluations coming from the company's control functions (e.g. Internal Audit), as well as any findings of the Bank of Italy in carrying out its own controls.

Below we detail the choices that the bank has made on the various relevant profiles (organisational set-up and operating/control procedures, due diligence, data retention, suspicious transactions) in order to ensure an overall internal control system for the prevention of money laundering and terrorist financing risks, capable of guaranteeing compliance with the laws and regulations on money laundering.

4.1. Organisational procedures and internal control measures

In application of the risk-based approach, the bank has put in place an organisational structure, operating and control procedures, and information systems that are suitable for ensuring compliance with statutory and regulatory provisions on money laundering and terrorist financing, in view of the nature, size and complexity of the business conducted, and the type and range of services provided.

To this end, the body with strategic supervisory functions:

- carries out an overall assessment, periodically updated, of its exposure to money laundering and terrorist financing risk, including at the Banking Group level;
- assigns the Group Anti-Money Laundering Service the responsibility for ensuring the adequacy, functionality and reliability of the anti-money laundering and anti-terrorism controls within the banking group;
- approves any delegation of responsibilities for suspicious transaction reporting, including with regard to the deputy of the delegate;
- entrusts the Internal Audit Department with the task of verifying the adequacy of the anti-money laundering and anti-terrorism organisational set-up and compliance with regulations.

In this context, the involvement of the corporate bodies and the proper fulfilment of the obligations incumbent upon them is crucial to mitigating the money laundering risk. Also for this reason, the composition of the corporate bodies must be such as to ensure the presence of adequate knowledge, skills and experience in order to understand the money laundering risks related to the bank's activity and *business* model.

4.2. Assessment of money laundering and terrorist financing risk factors and customer profiling

The bank applies customer due diligence measures proportionate to the extent of the money laundering and terrorist financing risks detected.

In order to calibrate the depth and extent of customer due diligence 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 regulatory provisions, the aim of which is to maximise the effectiveness of the company's controls and rationalise the use of resources.

The criteria used to determine the risk attributable to each customer take into account a number of factors, including the subjective characteristics of the customer, the executor and the beneficial owner, the nature of the relationships established with it, the type of transactions, supplemented by elements inferable from the subject's overall operations (such as the customer's behaviour, the reasonableness of the transaction, the geographical area, the distribution channel, etc.). In assigning the profile, the criteria laid down in the anti-money laundering decree, in the Bank of Italy's 'Provisions on adequate verification' and in the EBA Guidelines on risk factors are considered.

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

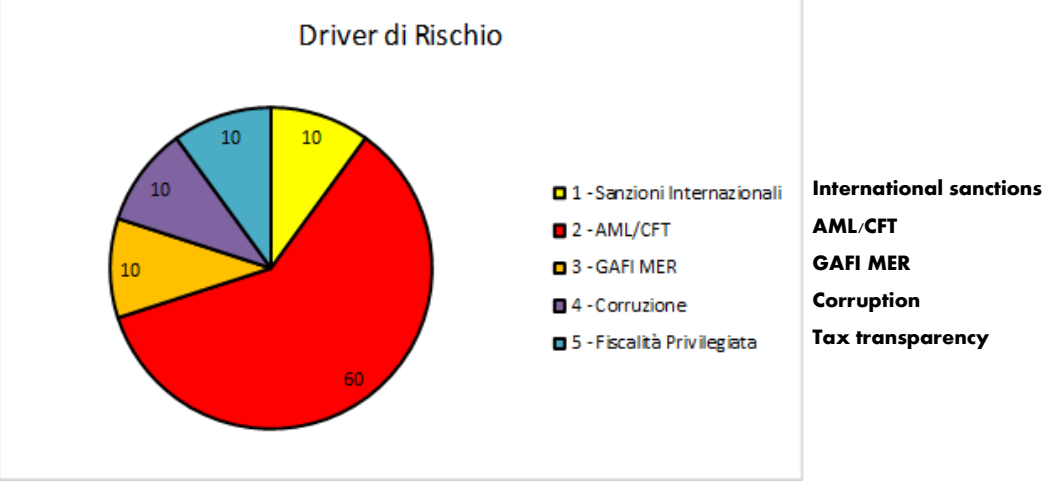
In assigning the profile, risk factors relating to:

- client (activities, area of operation, reputation, behaviour, links with high-risk persons or entities);
- countries and geographical areas (classification of countries; risk associated with Italian provinces classified as having a high crime rate);
- products, services and transactions (level of opacity, complexity, value, third party intervention, high use of cash);
- distribution channels (in-person or remote, use of agents/mediators).

With regard to the risk factors inherent in the country or geographical area in particular, the bank assesses:

1) the presence of financial sanctions, embargoes or measures related to the financing of terrorism or the proliferation of weapons of mass destruction, adopted by the UN, the EU, the US Treasury Department (so-called 'OFAC sanctions'), SECO (State Secretariat for Economic Affairs - Switzerland) and the United Kingdom (UK);
2) possible inclusion in lists of countries considered to be at 'high risk' of money laundering and terrorist financing, drawn up by authoritative sources ('black list' of the FATF; European Commission list of 'high risk' third countries);
3) the robustness of the anti-money laundering safeguards in place, as reflected in 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 assessed by authoritative and independent international organisations, such as *Transparency International* and the *Basel Institute on Governance*;
5) the level of tax transparency, as reflected in the reports endorsed by the OECD *Global Forum on* Tax Transparency and Exchange of Information and the assessments of the commitment to automatic exchange of information based on the so-called '*Common Reporting Standard* (or CRS)'; the possible inclusion in the EU list of non-cooperative jurisdictions for tax purposes is also relevant here.

The various geographic factors highlighted above assume the relative weight that can be seen in the following graph:



On the basis of these risk factors, 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 BPS AML office and circulated within the company and is also transmitted through the Group AML office to the subsidiaries for appropriate adjustments.

Information on the risk profile of money laundering and terrorist financing is made available to the operational structures in charge of the actual management and administration of customer relationships.

The lowering of a customer's risk level is only permitted by BPS's AML department in exceptional circumstances and is justified in writing.

At Group level, each Italian company assumes, for the same customer, the highest risk profile among those assigned by the Italian components of the Group.

4.3. Updating profiles and information acquired for customer due diligence

The bank monitors and periodically updates the scores and rules attributed to the risk profiling system, verifying the appropriateness of the risk class assigned in the event of events or circumstances likely to change the client's risk profile.

The timing and frequency of the update of the data and information acquired vary depending on the risk profile attributed; however, the update is carried out when it appears that the information previously acquired and used for due diligence is no longer current. In particular, it is carried out:

1) on the occasion of the opening of any new relationship with existing customers, regardless of their risk profile;
2) when changes, reported by the bank's automated procedures, have occurred with respect to
    a. expiry of identity documents and powers of representation;
    b. changes in beneficial ownership in the case of customers other than natural persons;

c. acquisition of qualities that can change the risk profile, detected by specific internal *screening* procedures, such as PEP or GDP status.

The table below shows the minimum frequency of updating of due diligence data, in relation to the risk profiles attributed to customers.

REFERENCE	RISK CLASS	MINIMUM UPDATE FREQUENCY
I	Irrelevant	A event - when information is no longer current
B	Low	A event - when information is no longer current
M	Medium	Every 24 months
A	High	Every 12 months

4.4. Customer due diligence procedures

The bank performs customer and beneficial owner due diligence with respect to the relationships and transactions inherent in the performance of its institutional activity:

1) on the occasion of the establishment of a continuing relationship;
2) on the occasion of the execution of an occasional transaction for an amount of €15,000 or more, irrespective of whether it is carried out in a single transaction or in several transactions that appear to be linked in order to carry out a split transaction;
3) if the bank acts as a conduit or is a party to the transfer of cash or bearer securities, in euro or foreign currency, for a total amount of €15,000 or more;
4) in all cases where:
   - there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold applicable;
   - there are doubts as to the completeness, reliability or truthfulness of the information or documentation previously acquired.

To ensure that customer due diligence is carried out properly, the bank proceeds:

a) identification of customers, possible executors, and beneficial owners;
b) verification of the identity of the customer, the executor (if any) and the beneficial owner 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 case of a high risk of money laundering and terrorist financing, of the occasional transaction;
d) constant monitoring of ongoing relationships, to update knowledge of the customer and the stated purpose of the relationship, to assess any unexpected, anomalous or inconsistent transactions with the customer's previously known economic and financial profile, or news of significant events;

e) updating the data and information collected, with the frequency depending on the risk profile previously associated with the customers.

The bank shall request from the customer, and the customer shall be required by law to provide under his own responsibility, all necessary and up-to-date information to enable it to fulfil its due diligence obligations.

Customer due diligence measures are proportionate to the extent of the money laundering and terrorist financing risks, taking into account specific factors relating to the customer, his conduct, the transaction, and the ongoing relationship.

Customer due diligence obligations are fulfilled with respect to both new customers prior to establishing a continuing relationship or executing an occasional transaction, and existing customers, when fulfilling the obligations laid down in Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and in the relevant national implementing legislation . Where the bank is unable to comply with the customer due diligence obligations, it shall not establish the continuing relationship, i.e. it shall not execute the transaction and, if the continuing relationship is already in place, it shall refrain from continuing it. In such a case, the bank also considers whether to send a suspicious transaction report, in the manner defined in the 'Suspicious Transaction Reporting Regulations'.

The concrete modalities for the identification and verification of customer, executor and beneficial owner data, for the acquisition and assessment of information on the purpose and intended nature of the continuing relationship and occasional transactions, and for ongoing monitoring during the course of the continuing relationship are governed by the AML Decree, the Bank of Italy's 'Provisions on Customer Due Diligence', the AML Handbook and the bank's further internal regulations, circulars and manuals on the subject.

4.4.1. Enhanced due diligence obligations

The bank applies enhanced customer due diligence measures where there is a high risk of money laundering and terrorist financing, either as a result of specific regulatory requirements or of its own assessment.

The bank considers the following high risk factors related to the customer, the executor, the beneficial owner, the products/services, the distribution channels, or geography:

a) continuing relationships established in abnormal circumstances, such as the client's or executor's reticence in providing the requested information or the unreasonableness of the transaction;
b) customers and/or beneficial owners resident or based in high-risk geographic areas;
c) negative reputational indicators relating to the customer, the beneficial owner and the executor;
d) structures qualifying as vehicles of asset interposition;
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 buyers, money changers, gaming/betting companies, both physical and *online*, agents and/or *money transfer* companies);
g) type of economic activity related to sectors particularly exposed to corruption risks;
h) activities of socially useful non-profit organisations (NPOs);
i) customer or beneficial owner identifiable as 'local Italian politicians' (PIL);
j) abnormal or excessively complex ownership structure in relation to the nature of the business;
k) services with a high degree of customisation, offered to customers with significant assets;
l) products or transactions that might favour anonymity or conceal the identity of the customer or beneficial owner. Examples include anonymous prepaid cards issued by foreign intermediaries, bearer shares, and transactions involving services related to the conversion of legal tender into virtual currency and vice versa;
m) frequent and unjustified cash transactions characterised by the use of large denomination euro banknotes, or by the presence of damaged or counterfeit banknotes;
n) transactions involving the transfer of cash or valuables from abroad for a total amount equal to or exceeding the equivalent of €10,000. In such cases, the bank shall request from the customer a copy of the cash transfer declaration provided for in Article 3 of Legislative Decree No. 195 of 19 November 2008, and shall investigate any refusal or reluctance on the part of the customer to provide the documentation;
o) payments received from third parties with no obvious connection to the customer or its business;
p) new-generation products and business practices, including the use of innovative distribution mechanisms or technologies for new or existing products;
q) the circumstance of having ceased for more than one year to hold one of the public offices provided for in Article 1(2)(dd)(1) of the AML Decree;
r) transactions relating to oil, weapons, precious metals, tobacco products, cultural artefacts and other movable property of archaeological, historical, cultural and religious importance or of rare scientific value, as well as ivory and protected species .

The bank always applies enhanced customer due diligence measures in the cases provided for by law, i.e:

1) relationships and occasional transactions involving high-risk third countries identified by the European Commission;
2) cross-border correspondent relationships, involving the execution of payments, with a correspondent banking or financial intermediary established in a third country;
3) ongoing relationships or occasional transactions with customers and their beneficial owners who have the status of politically exposed persons (PEPs), except where they act in their capacity as bodies of the public administration. In such cases, the bank adopts adequate

verification measures commensurate with the risk concretely identified , also taking into account the provisions of Article 23(2)(a)(2) of the AML Decree;

4) customers who carry out transactions that are characterised by unusually high amounts or in respect of which there are doubts as to the purpose for which they are, in practice, intended.

The authorisation process for opening/maintaining relationships with customers considered to be always high risk is outlined below:

TYPE OF RELATIONSHIP	AUTHORISATION
1. occasional relationships and transactions involving high-risk third countries identified by the European Commission	Head of Group Anti-Money Laundering Service
2. cross-border correspondent relationships, involving the execution of payments, with a correspondent banking or financial intermediary established in a third country	Managing Director, subject to the positive opinion of the Head of the Group Anti-Money Laundering Service; in the event that the Managing Director decides to depart from any negative opinion of the Anti-Money Laundering Officer, he/she shall justify such decision in writing, proposing appropriate measures aimed at mitigating the ML/FT risks highlighted by the Head of the Group Anti-Money Laundering Service
3. ongoing relations or occasional transactions with customers and their beneficial owners who are politically exposed persons (PEPs), except when they are acting in their capacity as bodies of public administrations	Senior management delegated for this purpose, subject to the positive opinion of the Head of the Group Anti-Money Laundering Service; if the senior management decides to depart from any negative opinion of the Anti-Money Laundering Officer, it must justify such decision in writing, proposing appropriate measures aimed at mitigating the ML/FT risks highlighted by the Head of the Group Anti-Money Laundering Service
4. customers who carry out transactions involving unusually large amounts or in respect of which there are doubts as to the purpose for which they are actually intended	Branch/unit manager

In addition, in the presence of one or more of the high-risk factors listed above - and where transactions deviate from what is normally expected, or are attributable to abnormal patterns of behaviour - the bank applies enhanced due diligence measures to relationships held by

5) *trust* or similar legal institution;
6) trust companies not registered under Article 106 of the Consolidated Banking Act;
7) agents and/or financial intermediaries engaged in *money transfer* activities;
8) companies operating in the gaming/betting sector, both physical and *online*;
9) non-profit organisations of social utility (ONLUS);
10) customers who have already been the subject of a suspicious transaction report in the previous three years and persons connected to them;
11) persons in respect of whom the bank has received notice of investigations or proceedings by judicial authorities or investigative bodies for money laundering offences in the preceding three years and persons associated with them;
12) PEPs-related entities;
13) customers resident or based in third countries assessed by the bank as high risk, according to the criteria outlined in section 4.2, or transactions involving those countries;

14) customers who, for objective reasons or due to further assessments by the relevant branch or other Group company, need to be subjected to enhanced measures.

The enhanced due diligence measures, which are in addition to the specific authorisation *procedures* provided for the cases set out in points 1), 2), 3) and 4) above, take the form of the acquisition of more information on the customer and on the beneficial owner, if any, and of a more accurate assessment of the nature and purpose of the relationship; a higher quality of the information requested; and an intensification of the frequency and depth of the analyses carried out as part of the ongoing monitoring of the relationship and of the transactions. In particular, these measures consist of:

i) in the acquisition of more information relating to the ownership and control structure of the customer. In particular, the documentation used to identify the beneficial owner must be dated no earlier than two years earlier;
ii) in acquiring more information on the continuing relationship, in order to fully understand its nature and purpose, in particular on:
    - the reasons why the customer asks for a particular product or service, especially if its financial needs could be better met in another way or in another country;
    - the origin and destination of the funds;
    - the nature of the business carried on by the customer and the beneficial owner;
iii) in a better quality of information to be acquired, such as:
    - verification of the origin of the client's assets and funds used in the ongoing relationship;
    - In the case of frequent and unjustified cash transactions, especially if carried out with large denomination banknotes, the bank shall investigate with the customer the reasons for such transactions;
iv) more frequent - at least annually - checks on ongoing relationships, in order to detect any suspicions of money laundering and terrorist financing at an early stage;
v) in the case of financial intermediaries engaged in *money transfer* activities, in the need to obtain the authorisation of the Head of the Group Anti-Money Laundering Service (or his delegate) for the opening or continuation of ongoing relationships;
vi) in the case of trusts and companies participated by trusts, the need to obtain the authorisation of the Group Anti-Money Laundering Officer (or his delegate) for the opening or continuation of ongoing relationships;
vii) In the case of cross-border correspondent banking relationships with banking or financial intermediaries in a third country, the bank applies, at the inception of the relationship, the enhanced due diligence measures set out in Article 25(2) of the AML Decree, in Section IV, Part Four of the Bank of Italy Due Diligence Provisions and in the Risk Factor Guidelines published by the EBA (Guideline No. 8).

4.4.2. Simplified due diligence measures

The bank may apply simplified customer due diligence measures in terms of the extent and frequency of compliance where there is a low risk of money laundering and terrorist financing.

The bank considers the following categories of customers or products/services to be low risk factors and therefore applies simplified due diligence measures:

1) companies admitted to listing on a regulated market and subject to disclosure requirements that impose an obligation to ensure adequate transparency of beneficial ownership, i.e. those listed on regulated markets in EU and non-EU countries recognised by Consob pursuant to Article 70 of the Consolidated Law on Finance;
2) public administrations, i.e. institutions or bodies performing public functions, in accordance with European Union law;
3) reports in the name of enforcement and insolvency proceedings;
4) customers resident or based in EU countries and in third countries with effective systems for the prevention of money laundering and terrorist financing, characterised by a low level of corruption or permeability to other forms of crime, an adequate level of tax transparency and commitment to the automatic exchange of information in tax matters, based on authoritative and independent sources;
5) banking and financial intermediaries referred to in Article 3(2) of the Anti-Money Laundering Decree - with the exception of those referred to in points (i), (o), (s) and (v);
6) Community banking and financial intermediaries;
7) banking and financial intermediaries based in a third country with an effective anti-money laundering and anti-terrorist financing regime, except in the case of cross-border correspondent relationships;
8) financial products or services appropriately defined and restricted to certain types of customers, aimed at fostering financial inclusion; this includes the 'basic current account' and loans by assignment of one-fifth of salary or pension and delegation of payment.

Simplified due diligence measures consist of:

i) the possibility of verifying the data relating to the beneficial owner by acquiring a confirmation statement signed by the customer, under his own responsibility;
ii) the absence of pre-established deadlines for updating the data collected for due diligence, except in cases where new relationships are opened, or when events occur that may increase the ML/TF risk profile of the customer.

In each case, the bank verifies the continued existence of the conditions for the application of the simplified procedure.

Simplified due diligence measures cannot be applied when:

- there are doubts, uncertainties or inconsistencies in relation to the identification data and information acquired in the identification of the customer, the executor or the beneficial owner;

- the conditions for the application of the simplified measures are no longer met, based on the risk indicators set out in the Anti-Money Laundering Decree and the provisions issued by the supervisory authorities;
- the monitoring of the customer's overall operations and the information acquired during the course of the relationship lead to the conclusion that a low-risk case does not exist;
- there is a suspicion of money laundering or terrorist financing.

4.4.3. Adequate verification in cases of remote operation

The bank takes care in the case of remote operations, by which is meant operations carried out by the customer without his physical presence (e.g. through computer communication systems).

Specifically, the bank, in cases of remote operations:

1) acquires the customer's and the executor's identification data and matches them against a copy, obtained by *fax*, mail or electronically, of a valid identity document;
2) performs additional checks on the data acquired, in one of the following ways:
   - transfer made by the customer through another intermediary established in Italy or in an EU country;
   - request for verification and confirmation of the data with another intermediary based in a SEPA ("*Single Euro Payments Area*") country, via SEDA ("*SEPA Electronic Database Alignment*") electronic messaging;
   - request to send countersigned documentation.

4.4.4. Third-party performance of due diligence obligations

The bank may use third parties for the fulfilment of customer due diligence obligations, without prejudice to its full responsibility for compliance with such obligations, in the manner and within the limits set by the Anti-Money Laundering Decree and the provisions of the supervisory authorities.

Under no circumstances may the bank use third parties based in high-risk third countries.

4.4.5. Constant monitoring during the ongoing relationship

The bank conducts ongoing monitoring during the course of the ongoing relationship to keep the customer's profile up-to-date and to identify inconsistencies that may constitute anomalies relevant for the purposes of taking enhanced due diligence measures, reporting suspicious transactions, and refraining from executing the transaction or continuing the relationship.

Ongoing control is exercised through the examination of the customer's overall operations, having regard both to existing ongoing relationships and to any specific transactions arranged, as well as through the acquisition of information when verifying or updating information for the

identification of the customer, the beneficial owner and the ascertainment and assessment of the nature and purpose of the relationship or transaction.

To this end, the bank adopts *ex-ante* and *ex-post* control procedures with a view to identifying, blocking and highlighting transactions suspected of money laundering and terrorist financing, and with regard to restrictions on the use of cash and bearer securities.

Controls are carried out on two levels:

- first-level controls, carried out by the branches/operational units that directly manage the relationship with the customer;
- second-level controls, carried out by the AML office of BPS, according to criteria and procedures governed by a specific control manual.

4.5. Obligations to abstain

If the bank finds it objectively impossible to carry out customer due diligence, it refrains from establishing the relationship or does not carry out the transactions and, in the case of existing relationships, terminates them. It also considers whether to file a suspicious transaction report with the FIU.

In any event, the bank shall refrain from entering into relationships or executing transactions and shall terminate the continuing relationship in the following cases:

1) correspondent accounts directly or indirectly traceable to *shell banks*;
2) legal persons to which trusts, trusts, limited liability companies (or controlled through bearer shares) established in high-risk third countries as identified by the European Commission in the exercise of its powers under Articles 9 and 64 of the Anti-Money Laundering Directive are directly or indirectly a party.

The bank also:

3) does not open anonymous reports or reports with fictitious/numerical headings;
4) does not offer *payable through accounts*;
5) refrains from offering products and/or services or carrying out operations that might favour anonymity;
6) refrains from establishing ongoing relationships or carrying out occasional remote transactions that are not assisted by adequate recognition mechanisms and procedures.

In implementing the provisions of the *Guidelines on Policies and Controls for the Effective Management of the Risks of Money Laundering and Terrorist Financing in Providing Access to Financial Services,* published by the *European Banking Authority* (EBA/GL/2023/04), and on the basis of the consequent amendments made to Legislative Decree No. 231/2007 by Law No. 136 of 9 October 2023. 136[9] , obliged entities shall ensure that the procedures adopted pursuant to Article 16 of the AML Decree ("Risk Mitigation Procedures") do not exclude, on a preventive and

[9] '*Conversion into law, with amendments, of Decree-Law No 104 of 10 August 2023, containing urgent provisions for the protection of users, concerning economic and financial activities and strategic investments*'.

generalised basis, certain categories of persons from offering products and services solely because of their potential high exposure to the risk of money laundering or terrorist financing (so-called "*derisking*").

In light of the foregoing, the bank does not enter into relationships with, or engage in occasional transactions with, companies that engage in activities as service providers relating to the use of virtual currencies (or cryptocurrencies), unless they can prove that they have adopted effective safeguards and procedures adequate to ensure the traceability of transactions, in order to exclude the anonymity of transactions.

4.6. Counter-terrorism and international embargo and fund transfer controls

In view of the growing importance of the fight against international terrorism, weapons of mass destruction development programmes, and trade in *dual-use* products and technologies, the bank adopts internal control procedures capable of identifying those customers or transactions that present a high risk of involvement in activities of a commercial or financial nature carried out by customers in violation of restrictive measures adopted by the international community against certain countries, natural and legal persons, entities, and organisations.

These checks, which are complementary to those carried out as part of ordinary due diligence procedures, can be divided into:

1) name checks: these are applied to the names of counterparties in the movement of funds, in order to ascertain that customers do not operate with persons subject to sanctions issued by international bodies involving the obligation to freeze funds and economic resources, or the application of restrictive measures of various kinds (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, SECO (State Secretariat for Economic Affairs, Switzerland) and the United Kingdom (UK) are considered;
2) country controls: these apply to transactions to and from countries considered at risk because: a) they have been identified by international bodies (FATF, European Union) as being exposed to a high risk of money laundering and terrorist financing; b) they have been assessed by international bodies (OECD, European Union) as having privileged tax status or as being uncooperative in the exchange of information on tax matters; c) they are subject to international embargoes, due to poor compliance with terrorist activity or violation of fundamental human rights;
3) Transactional controls on transactions: these apply to the funds transfer transactions carried out by customers and any underlying goods or services, to verify that embargoes or similar restrictions of a commercial (e.g. prohibitions or limitations *on the import/export of* goods, raw materials and technology) or financial (e.g. prohibitions or restrictions on financial services, investments, capital transactions) nature are not violated.

As a result of the checks carried out, where high-risk situations are identified, enhanced measures are put in place aimed at acquiring additional data and information, including through the production of appropriate documentation, and at monitoring with particular intensity the

evolution of the relationships belonging to the subject, without prejudice to the obligation to report suspicious transactions when the conditions exist.

In the specific circumstances indicated by the national and Community rules on embargoes, the obligations to freeze the funds and economic resources due to the persons or entities affected by the restrictive measures are also fulfilled, and with them the prohibition to make funds or economic resources available to them. The procedures of notification, communication or request for authorisation to the competent Authorities that may be provided for by the sanctions measures are also activated.

Finally, in compliance with the provisions of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, the bank adopts procedures capable of identifying the originator and beneficiary information that must be contained in transfers of funds.

4.7. Storage and making available of documents, data and information

The bank stores documents, data and information useful to prevent, detect or ascertain any money laundering or terrorist financing activities and to allow the analyses carried out by the competent authorities to be carried out by means of computerised storage systems that ensure

- the complete and timely accessibility of documents, data and information by the authorities;
- the timely acquisition of documents, data and information, including their date;
- the integrity of documents, data and information and that they cannot be altered after their acquisition;
- the adoption of appropriate measures to prevent any loss of documents, data and information;
- the transparency, completeness, clarity of documents, data and information and the maintenance of their historicity.

To this end, the bank shall ensure the retention of the documents, data and information acquired for ten years after the termination of the continuous relationship or the execution of the occasional transaction.

4.7.1. Types of documents, data and information to be kept

Pursuant to Article 31(2) of the Anti-Money Laundering Decree, the bank shall retain copies of the documents acquired during the due diligence of the customer, the executor and the beneficial owner.

The bank also keeps the following information:

1) with regard to continuing relationships: the operational point of establishment of the relationship, the date of establishment and the date of termination;
2) with regard to occasional transactions to be subject to due diligence and transactions

involving ongoing relationships: the date of execution, the amount, the monetary sign, the purpose of the transaction and the means of payment used;

3) With respect to occasional transactions for which due diligence is not required, the bank retains, in addition to the provisions of (2) above, the data and information capable of uniquely identifying the customer and the executor and, where known, the sector of economic activity and the data and information capable of uniquely identifying the beneficial owner.

The acquisition of 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 closing of the continuing relationship.

The retention obligations relate to ongoing relationships and transactions that are part of the bank's institutional business.

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

The bank shall make available to the Bank of Italy and the FIU, in accordance with the *standards* laid down in the Bank of Italy's "Provisions for the storage and making available of documents, data and information for combating money laundering and terrorist financing" of 24 March 2020, the data and information set out in Article 5 of those provisions.

4.7.3. Arrangements for storing and making available documents, data and information

For the storage of documents, data and information, the bank uses computerised storage systems, consisting of its accounting and management systems.

In order to ensure the traceability of customer transactions and to facilitate the performance of control activities, including inspections, by the Bank of Italy and the FIU, the bank ensures that data and information are made available to the Authorities through a specific standardised archive[10] , which complies with Appendix 2 of the Bank of Italy's "Provisions for the storage and making available of documents, data and information for combating money laundering and terrorist financing" of 24 March 2020.

4.7.4. Exemptions

Contrary to what was mentioned in the previous paragraph, the bank does not apply the provisions concerning the provision of data and information to the authorities through a specific standardised file in relation to ongoing relationships or transactions with:

1) the following banking and financial intermediaries referred to in Article 3(2) of the Anti-Money Laundering Decree, established in Italy or in another Member State;

[10] So-called 'ex AUI' (ex Archivio Unico Informatico), updated according to the new instructions mentioned above.

- banks;
- Poste italiane S.p.a.;
- electronic money institutions as defined in Article 1(2)(h-bis) TUB (IMEL);
- payment institutions as defined in Article 1(2)(h-sexies) TUB (so-called IP);
- securities brokerage companies, as defined in Article 1(1)(e), TUF (SIM);
- asset management companies, as defined in Article 1(1)(o) TUF (SGR);
- investment companies with variable capital, as defined in Article 1(1)(i) TUF (SICAVs);
- investment companies with fixed capital, securities and real estate, as defined in Article 1(1)(i-bis) TUF (SICAF);
- intermediaries registered in the register provided for in Article 106 TUB;
- Cassa Depositi e Prestiti S.p.A;
- insurance undertakings, operating in the classes referred to in Article 2(1), CAP;
- micro-credit providers, pursuant to Article 111 TUB;
- confidi and other entities referred to in Article 112 TUB;
- Established branches of banking and financial intermediaries (as referred to in the preceding paragraph), having their registered office and head office in another Member State or in a non-Member State;
- banking and financial intermediaries (as referred to in the previous point) having their registered office and head office in another Member State, established without a branch in the territory of the Italian Republic;

2) the persons referred to in Article 3(8) of the Anti-Money Laundering Decree[11] ;
3) the provincial state treasury and the Bank of Italy.

4.8. Suspicious transaction reporting

The bank sends a suspicious transaction report to the FIU, reasonably prior to carrying out the transaction, when it has knowledge, suspicion or reasonable grounds to suspect the existence or attempted existence of money laundering or terrorist financing or that the funds of the transaction are derived from criminal activity. The suspicion is inferred from the characteristics, size, and nature of the transactions, also taking into account the economic capacity and activity of the person to whom it is reported.

The frequent and unjustified use of cash transactions and the withdrawal or deposit of cash in amounts inconsistent with the client's risk profile constitute elements of suspicion.

The management of the process that may lead to the reporting of a suspicious transaction is attributed to the suspicious transaction reporting officer, who

[11] Central securities depositories, 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, companies managing clearing and guarantee systems for transactions in financial instruments.

- evaluates, in the light of all available elements, the suspicious transactions detected;
- transmits to the FIU any reports it deems to be well-founded;
- file reports deemed unfounded;
- keeps evidence of the assessments made under the procedure, even if the report is not sent to the FIU.

The bank guarantees all appropriate measures to ensure the confidentiality of the identity of persons reporting a suspicious transaction. In particular, the name of the person making the report may never be disclosed, unless the judicial authorities deem this to be indispensable for the purpose of ascertaining the offences for which proceedings are being conducted. In any case, the provisions of Article 38 of the Anti-Money Laundering Decree ("Protection of the reporter") apply.

It is also forbidden, for the persons required to report a suspicious transaction and for anyone who has knowledge of it, to give notice to the customer concerned or to third parties of the fact that a report has been made, of the sending of further information requested by the FIU or of the existence and/or possibility of investigations into the matter. In relation to the processing of personal data in connection with the reporting and communication activities referred to in this paragraph, the rights set out in Articles 15 to 18 and 20 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 shall be exercised within the limits provided for in Article 2-undecies of Legislative Decree No 196 of 30 June 2003, as amended.

The reporting of suspicious transactions, made in good faith by the bank, its employees or directors, does not constitute a breach of any reporting restrictions imposed by contract with the customer or by any legislative, regulatory or administrative provisions; moreover, it does not give rise to liability of any kind, even in cases where the reporting party has no knowledge of the underlying criminal activity and regardless of whether the illegal activity was actually carried out.

4.9. Staff Training

Effective application of anti-money laundering and anti-terrorism legislation requires adequate knowledge of the obligations and responsibilities that may arise from non-compliance. Hence the need for appropriate training and continuing education measures for all personnel, with programmes that take into account developments in national and international legislation and internal self-regulation (regulations, manuals, procedures, circulars, etc.).

To this end, the bank organises staff education and training programmes and ensures the dissemination of a corporate culture of compliance.

The Chief Executive Officer establishes annually, in cooperation with the Group Anti-Money Laundering Service and the Personnel and Organisational Models Service, training and education programmes for personnel on the obligations laid down in the anti-money laundering regulations 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 or are otherwise involved in the process of reporting suspicious transactions, as well as those belonging to the Group Anti-Money Laundering Service, who are required to be constantly updated on the evolution of money laundering risks and the typical patterns of criminal financial transactions;

- ensure that staff are kept up-to-date on regulatory developments and the risks of money laundering and terrorist financing;
- are carried out periodically and systematically and are submitted annually for approval to the body with management function.

The bank ensures that the procedures for internal reporting of violations under Article 48 of the Anti-Money Laundering Decree (so-called '*whistleblowing*') are brought to the attention of all personnel. This task is currently assigned to the Compliance Officer and DPO.

4.10. Information flows

With specific reference to information flows to the FIU, the bank transmits:

- aggregated data concerning its operations, in order to allow the carrying out of analyses aimed at bringing to light possible money laundering or terrorist financing phenomena within certain territorial areas, in accordance with the procedures and timeframes defined by the Authority itself in the "Provisions for sending aggregated data" of 25 August 2020 (so-called S.AR.A. flows);
- within thirty days from the date of entry into force of EU regulations or decrees issued by the Ministry of Economy and Finance, on the freezing of funds and economic resources held by natural or legal persons, groups or entities engaged in conduct aimed at terrorist acts or the financing of weapons of mass destruction or the threat to international peace and security, the measures applied, indicating the persons involved, the amount and nature of the funds or economic resources;
- promptly, transactions, relationships and any other available information attributable to the persons designated or those in the process of being designated in EU regulations or decrees issued by the Ministry of Economy and Finance.

With regard to internal reporting within the bank and the banking group, the bank has defined the flows that corporate structures must exchange in order to ensure the necessary alignment with regard to the control of money laundering and terrorist financing risks, detailed in Appendix 1 ("Internal Information Flows") and Appendix 2 ("Intra-Group Flows").

The Group Anti-Money Laundering Service has access to all the bank's activities and to any information relevant to the performance of its duties, including through direct interviews with staff. To this end:

- the bank's other structures and/or functions must communicate to it, in a timely and complete manner, any facts that are relevant for the purposes of controlling the risks in question;

- may request and receive from other structures and/or functions any further information relevant to the performance of its tasks.

4.11. Reporting Obligations of the Board of Auditors and Violation Reporting Systems

The Board of Statutory Auditors monitors compliance with the legislation on money laundering and terrorist financing. To this end, it notifies the Bank of Italy without delay of all facts of which it becomes aware in the performance of its duties that may constitute serious or repeated or systematic or multiple breaches of the provisions laid down by law and implementing provisions.

If, in the course of his duties, he becomes aware of potentially suspicious transactions, he shall inform the reporting officer and the Group Anti-Money Laundering Service.

The bank also has specific procedures for the internal reporting by employees and associates of potential or actual violations of the provisions laid down to prevent money laundering and terrorist financing (*whistleblowing*).

5. SELF-ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS AND ANNUAL REPORT

In accordance with the criteria and methodologies set out in the Organisation, Procedures and Controls Provisions issued by the Bank of Italy and the "Guidelines on Policies and Procedures for Compliance Management and the Role and Responsibilities of the Anti-Money Laundering Officer" issued by the EBA, the bank conducts a self-assessment of the money laundering (ML) and terrorist financing (FT) risk to which it is exposed.

The self-assessment is conducted on the basis of a methodology comprising the following macro-activities and aspects:

a) Identification of inherent risk (on a four-value rating scale): current and potential risks to which the bank is exposed are identified, also taking into account elements provided by external information sources. In particular, factors such as the type of clientele, products and services offered, the bank's operations, distribution channels and geographical area are taken into account at this stage;

b) vulnerability analysis (on a four-value rating scale): in this phase, the adequacy of the organisational set-up and of the prevention and monitoring controls are analysed with respect to the risks previously identified in order to identify any vulnerabilities; the attribution of the vulnerability level is accompanied by an overall judgement on the effectiveness of the controls in place as well as a brief illustration of any weaknesses identified, with an explanation of the reasons for the score;

c) determination of residual risk (on a four-value rating scale): the bank assesses, depending on and in relation to the line of *business*, the level of residual risk to which it is exposed in view of the level of inherent risk and the robustness of the mitigation safeguards, using the residual risk determination matrix developed by the Bank of Italy;

d) remedial action: once the residual risk has been determined, the bank defines appropriate remedial action and remedies to be taken to address any existing critical issues, as well as the adoption of appropriate AML prevention and mitigation measures.

As far as the Banking Group is concerned, the Head of the Group Anti-Money Laundering Service coordinates the exercise carried out by each of the Group companies and conducts a Group self-assessment exercise, the results of which are assessed by the Board of Directors, after examination by the Control and Risk Committee, the Board of Statutory Auditors, the Internal Audit Service and the Risk Control Service.

The self-assessment exercise, referring both to the Parent Company and to the Banking Group as a whole, together with the Parent Company's annual report, is updated annually by the Group Anti-Money Laundering Service and is transmitted to the Bank of Italy by 30 April of the year following the year of assessment. It is also promptly updated when significant new risks emerge or significant changes occur in existing risks, operations or organisational or corporate structure.

Furthermore, the results of this activity contribute to the definition of the *Risk Appetite Framework of* the Bank and the Banking Group.

The annual report must include the following information

1) as part of the ML/FT risk assessment:
    a. a summary of the main findings of the risk assessment at business area level; whether an update to this effect was carried out in the previous year; whether supervisory authorities have requested updates in this regard;
    b. description of any changes related to customer profiling criteria, highlighting whether they are in line with the ML/FT risk assessment of the company's business;
    c. classification of customers according to risk and indication of the number of customers, broken down by risk band, in relation to which the review and update of due diligence has not yet been completed;
    d. statistical data concerning:
        i. number of anomalous transactions detected;
        ii. number of anomalous transactions analysed;
        iii. number of suspicious transaction reports forwarded to the FIU, broken down by country where the transactions took place;
        iv. number of reports closed due to AML/CFT anomalies;
        v. number of requests for information received from the FIU, judicial authorities and law enforcement agencies;
2) with regard to resources:
    a. description of the organisational structure of the Group Anti-Money Laundering Service;
    b. description of the human and technical resources assigned to the Group Anti-Money Laundering Service;
    c. where present, list of outsourced AML/CFT processes and description of the supervision carried out;
    d. description of completed AML/CFT training activities and training plan for the following year;
3) on policies and procedures:
    a. summary of the most important measures and procedures adopted during the year, including recommendations, problems, shortcomings or irregularities identified;
    b. control actions taken to assess the implementation of AML/CFT policies, controls and procedures by employees, agents, distributors, etc., as well as the adequacy of control tools employed by the bank for AML/CFT purposes;
    c. Group AML activity plan for the following year;
    d. findings of internal and external AML/CFT reviews and any progress made against

them;

e. supervisory activities carried out by the competent authorities, violations identified and any sanctions imposed, together with the actions taken to remedy the violations identified, with the relevant status.

Using the same methods, the head of the Group Anti-Money Laundering Service prepares a summary interim (half-yearly) report, including the self-assessment of ML/FT risks, the results of which are assessed by the Board of Directors, after examination by the Control and Risk Committee, the Board of Auditors, the Internal Audit Service and the Risk Control Service.

Below is the outline of the annual report according to Bank of Italy guidelines:

1	Description and location of the anti-money laundering function in the company (or group) organisation, including changes during the year, human and technical resources assigned and processes outsourced
2	Activities of the anti-money laundering function during the reporting period, any dysfunctions detected and related corrective actions in the sectors:
	a. of due diligence and customer profiling. In this context, specific information should be provided on: any delays in completing due diligence, including failure to identify the beneficial owner; the distribution of customers (in absolute terms and as a percentage of the existing customer base) among the different risk classes
	b. data retention
	c. the process of identifying and reporting suspicious transactions (indicating the number of reports sent to the FIU during the year and those assessed and filed)
	d. the identification and enforcement of international financial sanctions against terrorism and the proliferation of weapons of mass destruction
3	Money Laundering Risk Self-Assessment Exercise
4	Adaptation initiatives defined in the light of the findings of the money laundering risk self-assessment exercise and their status
5	Training activities implemented in the reporting period and planned for the following year
6	Any problems specific to the intermediary and other relevant information
7	Plan of activities of the anti-money laundering function for the following year
8	Number of customer relationships closed due to AML anomalies
9	Any malfunctions ascertained by other internal control functions and corrective measures implemented
10	Communications with the supervisory authority, including sanctions imposed and corrective actions requested by the latter
11	Number of requests for information received from the FIU, judicial authorities and law enforcement agencies

Annex 1 - INTERNAL INFORMATION FLOWS

INFORMATION FLOW	SENDER	WAYS	DESTINATORY	PERIODICITY
1. Annual report and self-assessment	Group Anti-Money Laundering Service	• Via the anti-money laundering officer	• Board of Directors • Audit and Risk Committee • Board of Auditors • Internal Audit Service • Chief Risk Officer	Annual
2. Half-yearly Operations Report and Interim Self-Assessment	Group Anti-Money Laundering Service	• Via the anti-money laundering officer	• Board of Directors • Audit and Risk Committee • Board of Auditors • Internal Audit Service • Chief Risk Officer	Half-yearly
3. Reports of breaches or significant shortcomings encountered in the performance of the relevant duties and on infringements pursuant to Article 46(1)(b) and Article 51(1) of Legislative Decree No. 231/2007, for subsequent communication to the Supervisory Authority or to the MEF	Group Anti-Money Laundering Service	• Directly	• Board of Directors • Audit and Risk Committee • Board of Auditors • Supervisory body	A event
4. Group Quarterly Indicators	Group Anti-Money Laundering Service	• Directly	• Managing Director • Anti-Money Laundering Officer • Audit and Risk Committee • Board of Auditors • Chief Risk Officer • Head of Internal Audit	Quarterly
5. Information on specific requests from supervisory authorities	Group Anti-Money Laundering Service	• Through the person responsible for anti-money laundering	• Board of Directors • Audit and Risk Committee • Board of Auditors	A event
6. Risk assessment related to the introduction of new products and services, significant modification of products or services already offered, entering a new market or starting new activities	Group Anti-Money Laundering Service	• Directly	• Managing Director	A event
7. Reports of second-level audits where irregularities or failures in AML/CFT risk control measures were found, including at the Banking Group level	Group Anti-Money Laundering Service	• Directly	• Managing Director • Anti-Money Laundering Officer • Board of Auditors • Audit and Risk Committee • Head of Internal Audit • *Chief Risk Officer*	A event
8. Reports of audits in which irregularities or failures in AML/CFT	Internal Audit Service	n.a.	• Managing Director • Anti-Money Laundering Officer • Board of Auditors	A event

INFORMATION FLOW	SENDER	WAYS	DESTINATORY	PERIODICITY
risk control measures were found, including at banking group level			• Head of Group Anti-Money Laundering Service; • Head of the Group AML office; • Head of the BPS AML office	

Annex 2 - INFORMATION FLOWS INFRA GROUP

INFORMATION FLOW	SENDER	DESTINATORY	PERIODICITY
1. Annual report and self-assessment	subsidiary's anti-money laundering structure	• Group Anti-Money Laundering Service • BPS and Group Anti-Money Laundering Officer	Annual
2. Half-yearly Operations Report and Interim Self-Assessment	subsidiary's anti-money laundering structure	• Group Anti-Money Laundering Service • BPS and Group Anti-Money Laundering Officer	Half-yearly
3. Risk indicators established by the Group Anti-Money Laundering Service	subsidiary's anti-money laundering structure	• Group Anti-Money Laundering Service • BPS and Group Anti-Money Laundering Officer	Monthly
4. Significant anomalies, violations or deficiencies reported	subsidiary's anti-money laundering structure	• Group Anti-Money Laundering Service • BPS and Group Anti-Money Laundering Officer	A event
5. Minutes of audits where irregularities or failures in the AML/CFT control of subsidiaries were found	Internal audit	• Managing Director • BPS and Group Anti-Money Laundering Officer • Board of Auditors • Group Anti-Money Laundering Service	A event