Gruppo Banco Desio
Dal 1909

ANTI-MONEY LAUNDERING

and

ANTI-TERRORISM FINANCING POLICIES

First version of the document	30 April 2013
First update	28 April 2015
Second update	29 November 2016
Third update	30 May 2017
Fourth update	21 September 2017
Fifth update	11 July 2019

Gruppo Banco Desio
Dal 1909

CONTENTS

1 INTRODUCTION AND PURPOSES OF THE DOCUMENT

The aim of this document (hereinafter also referred to as the "Policy") is to establish the policies of Banco di Desio e della Brianza (hereinafter also referred to as the "Bank") to manage the risks of money laundering and terrorism financing, in compliance with the provisions of Italian law (hereinafter also referred to as the "Anti-Money Laundering Decree") and with the provisions of the Measure issued by the Bank of Italy in March 2019 relating to the organisation, procedures and internal controls (hereinafter also referred to as the "Measure") that banking and financial intermediaries, including this Bank, must comply with.

The organisational structure, operating procedures and controls, as well as information systems, are structured taking into account the nature, size and complexity of the business carried on and of the type and range of services supplied.

As a result, based on the criterion of proportionality and the risk-based approach, this Policy defines the following, which is in line with the requirements of national legislation and is consistent with the business model and the organisational structure adopted, with the sales policies pursued and with the risk of money laundering to which the Group is currently exposed, as revealed by the last self-evaluation conducted:

- the general principles of the risk and strategic policy management model;
- operating procedures and guidelines for the concrete management of the risk of money laundering and terrorism financing;
- the responsibility and duties of the Company Bodies and the corporate departments.

The Policy establishes the minimum standards that managers, executives and employees (together the "employees") must comply with when doing their jobs.

More specifically, it aims to:

- hold the employees and external staff to account;
- clearly define the roles, duties and responsibilities at the various levels on the subject of monitoring the money laundering and terrorism financing risk;
- assign the duty of supervising – at group level - the commitment to preventing and managing the risks in question to a specific company department;
- establish a control function structure with coordinated components, including through suitable flows of information (established in the Group Information Flow Regulation), and that is also consistent with the organisation of the system, the complexity, the company size, the type of services and products available and the extent of the risk that could be associated with the types of Customers, the kind of services and products offered and the distribution channel;
- establish a control system that aims to ensure compliance with internal procedures and all regulatory obligations by staff and external staff, with special regard to the "active collaboration" and continued analysis of customer operations.

Pursuant to the aforementioned Bank of Italy Order, the Policy is defined by the General Manager and is submitted to the approval of the Board of Directors together with the grounds for the choices of the organisational and procedural structures and the internal controls made in it. The document is constantly updated and is reviewed at least once a year based on the outcome of the self-assessment conducted by the Anti-Money Laundering function and is made available with full circulation to the employees, also through publication on the corporate intranet.

The Policy, together with the Code of Ethics, Anti-Money Laundering Process Regulation and Operating Manual - which describe in detail the internal operating procedures - is one of the controls provided in accordance with the Company Organisational Model adopted by the Bank pursuant to Legislative Decree 231/2001 (MOG 231).

2 DEFINITIONS AND GENERAL PRINCIPLES

2.1 Notion of Money Laundering and Terrorism Financing

The laundering of money derived from unlawful actions is one of the most serious crimes on the financial market. The reinvestment of unlawful proceeds into legitimate assets profoundly changes market mechanisms, invalidates the efficiency and fairness of the financial assets and weakens the economic system. The risk of money laundering or financing terrorism in financial institutions is expressed in the form of involvement in these situations, including involuntary.

The prevention law defines money laundering as any activity aimed at using the proceeds of criminal activity with the intention of concealing or disguising the origin.[1]

Art. 2 of Italian Legislative Decree 231/2007 specifies that in order to prevent and fight the use of the economic and financial system for the purpose of money laundering and terrorism financing:

- the term **Money Laundering** means:

  a) the conversion or transfer of goods, carried out with the awareness that they originated from criminal activity or participation in criminal activity, in order to conceal or disguise the unlawful origin of the goods or to help anyone who may be involved in those activities to evade the legal consequences of their actions;
  b) the concealment or disguising of the real nature, origin, location, provision, movement, ownership of the goods or the rights to them, made with the awareness that said goods originated from a criminal activity or from participation in this type of activity;
  c) the acquisition, holding or use of goods with the awareness, at the time of receipt, that said goods come from a criminal activity or participation in this type of activity;
  d) participation in one of the offences set out under the previous letters, conspiracy to commit this type of offence, the attempt to commit it, aiding, abetting, facilitating or counselling anyone to commit it.

- the term **Financing Terrorism** means:

any activity aimed, by all means, at gathering, supplying, brokering, depositing, safekeeping or providing funds or financial resources, in any manner, aimed at being, in whole or in part, used to carry out one or more crimes for terrorism purposes, as provided under the criminal laws, regardless of the actual use of the funds or financial resources to commit the aforementioned crimes[2].

---

1 This definition of money laundering that comes from the adoption of the EU directives is broader than the one provided for repressive purposes in the Italian Criminal Code, which states:

Art. 648 bis Criminal Code - Money Laundering.

"*Except in cases of participation in the crime, whoever replaces or transfers money, assets or other benefits coming from a crime committed with criminal intent, or commits other transactions in connection with them in such a way as to obstruct the identification of their criminal origin, is punished with imprisonment from four to twelve years and with a fine from Euro 5,000 to Euro 25,000.*
The penalty will be increased if the action is committed during the performance of a professional activity. The sentence is reduced if the money, assets or other benefits originate from a crime punishable with imprisonment of less than the maximum of five years. The last paragraph of Art. 648 applies."

Italian Law no. 186 of 15 December 2014 introduced the crime of self-laundering into the Criminal Code.

Art. 648-ter.1 Criminal Code - Self-laundering.

"A sentence of imprisonment from two to eight years and a fine of Euro 5,000 to Euro 25,000 will be imposed on anyone who, having committed or helped perpetrate a crime committed with criminal intent, uses, replaces, or transfers the money, assets or other benefits derived from the commission of said crime into economic, financial, entrepreneurial or speculative assets in order to actually prevent identification of the criminal origin.
A sentence of imprisonment from one to four years and the penalty of Euro 2,500 to Euro 12,500 will be imposed if the money, assets or other benefits originate from a crime committed with criminal intent, punishable with imprisonment of less than the maximum of five years.
In any case, the sanctions provided under the first paragraph will be imposed if the money, assets or other benefits originate from a crime committed with the conditions or purposes set out under article 7 of law decree 152 of 13 May 1991, converted, with amendments, by law 203 of 12 July 1991, as amended.
Apart from the cases set out in the previous paragraphs, actions where the money, assets or other benefits are to be merely utilised or for personal enjoyment are not subject to sanction. The penalty will be increased if the actions are committed during the performance of banking or financial activities or any other professional activity. The sanction will be reduced by up to a half if anyone has effectively acted to prevent the conduct from leading to further consequences or to guarantee evidence of the offense or identification of the assets, money or other benefits resulting from the crime."

2 Pursuant to Art. 1, par. 1, letter f) of Italian Legislative Decree 109/2007, the term funds means financial assets and benefits of any kind, also owned through third parties that may be natural persons or legal entities, including, purely by way of esample: payment instruments; 2) deposits at financial entities or other parties, account balances, receivables and obligations of any nature; 3) transferable securities at public or private level and financial instruments as defined by Art. 1, par. 2 of the Financial Consolidation Act, pursuant to Italian Legislative Decree no. 57 of 24 February 1998; 4) the interest, dividends or other income and value increases generated by the assets; 5) the credit, right of set off, guarantees of any types, deposits and other financial commitments; 6) letters of credit, bills of lading and other

Both the money laundering and the financing of terrorism involve the handling di cash flows. However, both activities have different ends: essentially, money laundering is an activity aimed at transferring or transforming proceeds which originated from unlawful activities into lawful resources with the consequent difficulty in reconstructing the criminal origin of the money flow (the aim pursued is to disguise or conceal the historic origin of the money that was transferred); on the other hand, the financing of terrorism aims to allocate the money towards a specific unlawful activity.

In accordance with the FATF recommendations and the IV Anti-Money Laundering Directive issued by the European Parliament and the Council on 20 May 2015[3], which include "tax crimes" (related to direct and indirect taxes) among the crimes that lend themselves to money laundering activities[4], the Bank considers these phenomena both in monitoring risks and in applying measures of active collaboration.

In the context described, the role that the financial intermediaries carry out - and they may even be unaware that they are doing it - is highly sensitive due to the type of services offered. Criminal proceeds could be made pass through the legitimate channels of the services offered by financial operators, who would in this case would find themselves, also involuntarily. aiding money laundering through the products and services offered. In order to prevent the actual use of financial intermediaries in relation to these activities, the law requires full awareness of the risks associated with the activity actually performed by the financial intermediaries, an in-depth knowledge of their customers, and it sets specific obligations for banks for managing the money laundering and terrorism financing risk.

2.2 Risk of money laundering and terrorism financing

In the classification of risks defined by the prudential regulations[5], money laundering and terrorism financing risks mainly fall under legal and reputational type risks. The Banco Desio Group adopted a specific "company risk management policy" to monitor said risk. It specifically includes the "Policy for managing operational risks" and the "Policy for managing reputational risks".

There are a number of different aspects to the risk of money laundering:

- risk of recurrence of the crime of money laundering and self-laundering by third parties who use the intermediary and the financial system for criminal purposes;
- risk of participating or assisting, even unwittingly, in the crime of money laundering and self-laundering by third parties on behalf of negligent, and collaborating or disloyal employees (wilful nonfeasance in the possible failure to report the transaction that proved to be suspicious, failure to apply the internal dispositions / internal monitoring supervision of negligence or fraud);
- risk of inadequacy of the organisational model, internal procedures and the control system;
- risk of malfunction of the computer procedures, or inadequacy of the technological infrastructure.

The risk of money laundering and financing terrorism is always associated with reputation risks, even significant, for the intermediary.

2.3 Main obligations provided by the regulations to combat money laundering and the financing of terrorism

The Anti-Money Laundering Decree and related implementing rules provide for specific provisions for the recipients that are aimed at fighting money laundering and terrorism financing phenomena. The most important fulfilments, obligations and prohibitions that the Bank and the Group must observe are summarised hereunder:

- **Customer due diligence** - set of fulfilments in order to correctly identify the money laundering and terrorism financing risk of the customers and therefore evaluate whether to go ahead with the transaction or not and/or

certificates representing goods; 7) documents proving an equity interest in funds or financial resources; 8) all other export finance instruments. 9) insurance policies concerning the life segments pursuant to Art. 2, par. 1 of Italian Legislative Decree No. 209 of 7 September 2005 carrying the Private Insurance Code.

3 EU Directive 2015/849 of the European Parliament and Council of 20 May 2015 concerning the prevention of the use of the financial system for money laundering activities or the financing of terrorism, which modifies the (EU) regulation no. 648/2012 of the European Parliament and Council and revokes directive 2005/60/EC of the European Parliament and Council and directive 2006/70/EC of the Commission.

4 *Cfr*. See FATF recommendations of February 2012 (International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FAFT Recommendations).

5 *Cfr*. Circular by Bank of Italy No. 263/2006.

opening/maintain the customer accounts. The bank is required to comply with these obligations in the following cases:

a) when an account is being opened;
b) when it is carrying out occasional transactions, ordered by customers which involve the sending or movement of payment means for amounts equal to or higher than Euro 5,000, regardless of whether they are carried out as a single transaction or as more than one transaction with the transactions appearing to be related to carry out a transaction that is split into parts, or that consists of a transfer of funds, as defined by Art. 3, par. 1, point 9 of (EU) Regulation no. 2015/847 of the European Parliament and of the Council, higher than Euro 1,000;
c) when there is a suspicion of money laundering or terrorism financing;
d) when there are doubts regarding the truthfulness or adequacy of the data obtained previously to identify the customers.

Effectively, it involves a more extended duty of customer due diligence, to be carried out by acquiring information and backing documentation on the customer, beneficial owner of the account, representative and the nature and scope of the business relations, the origin / destination of the funds, that involve continuous monitoring of the customer's transactions. The ability to assess the level of risk and thus enable the type of conduct and the organisational solutions called for in each case each occasion to be more flexible, entails a greater awareness and responsibility on behalf of all personnel, which must engage in continuous training, and means that appropriate procedures, instruments and controls have to be employed, the validity and effectiveness of which is subject to control by the Supervisory authorities.

- **Filing obligations** – the Bank files the data and information required by the Anti-Money Laundering Decree mainly through the Centralised Computer Archive (hereinafter called, for the sake of brevity: AUI) already established pursuant to legislation previously in force. The data and information must be promptly recorded in a transparent, complete and clear way, and in any case, no later than the thirtieth day following completion of the transaction. The data and information are kept for ten years from the date the account is closed / the occasional transaction is executed.

- **Reporting of suspicious transactions (SOS) -** to be forwarded without delay to the Financial Information Unit (hereinafter called, for the sake of brevity: FIU) when the Bank knows, suspects or has reasonable grounds for suspecting that there are money laundering or terrorism financing activities being carried out, or that were carried out or that are being attempted, or that in any case the funds, regardless of their amount, come from criminal activity.

- Adoption of measures aimed at ensuring the **confidentiality of the identity** of the parties that make the report;

- **Sending the aggregate data flows (S.A.R.A.)** concerning the operations undertaken at each Branch / local office **to the FIU** every month so that targeted analyses can be made as to make any money laundering or terrorism financing activity emerge in specific geographical regions.

- Sending the **Objective Communications to the FIU** every month according to the methods and standards set out in the regulatory provisions in force[6].

- **Prohibition on transferring money and bearer securities** between different parties and for any reason for amounts that exceed the limits established by Italian law and the associated **obligation to report** any breaches **to the Ministry for Economy and Finance.**

- **Training obligations**, which the Bank will guarantee to all company levels, through adequate and continuous education aimed at teaching the obligations and the significance of the Anti-Money Laundering procedures and to promote a relevant risk prevention culture.

- **Fight against terrorism financing** – the Bank adopts **measures** aimed at fighting national and international financing of terrorism and has procedures and **systems** aimed at **preventing and avoiding the establishment** (or

6 The Measure that regulates this type of finding (Objective Communications) was issued by the FIU in accordance with the Financial Security Committee on 28 March 2019.

continuation, if already existing) **of accounts** and **the carrying out of transactions** with subjects suspected or responsible for terrorist activities.

2.4 General principles of the money laundering and terrorism financing risk management model adopted by the Group

In order to ensure correct compliance with the requirements to combat money laundering and the financing of terrorism, the Group actually:

- has adopted **processes, instruments and controls** based on the 'risk-based approach' principle, to ensure full compliance with the principles contained in this Policy;
- ensures adequate, complete and timely **information flows** to and from the company bodies, top management and the control and operating Units, as well as between the Parent Company and the subsidiary companies;
- ensures training and **instruction** programs to keep employees fully up-to-date;
- if it makes use of **financial consultants and financial business agents** to carry out its corporate activities, it requires that they:
  - comply with this Policy and with the internal regulations relating to anti-money laundering and combating terrorism financing;
  - adopt the information tools placed at their disposal by the Bank in order to meet their obligations;
  - take steps so that the Bank acquires an adequate, complete and updated wealth of information on the customers collaborate with the Group Branches in those cases in which the Bank plans to take strengthened measures of adequate verification;
  - meet the reporting and active collaboration obligations;
  - has adopted a **231 Organisational model**, implementing the provisions of Legislative Decree no. 231 of 2001, to identify possible areas where the commission of the presumed offences could be imagined in relation to the activity carried out, including terrorism-related offences or subversion of democracy (pursuant to Article 25-quater Legislative Decree 231/2001) or the offences of receiving stolen goods, money laundering, use of money, goods or benefits of unlawful origin or self-laundering (pursuant to Article 25-octies of Legislative Decree 231/2001):
    All Bank personnel and collaborators must strictly comply with the prohibitions and warnings provided under the Code of Ethics regarding relations with parties with whom there is a reasonable suspicion that they could be involved in unlawful activities;
- carries out a **self-assessment** of one's **exposure to the risk** of money laundering and financing of terrorism activities (so called Self-assessment Exercise) and drafts a plan of action designed to rectify any anomalies or weaknesses that may have been found or the reinforcement of existing verifications.
  To this end it has approved – in line with the instructions distributed by the Bank of Italy[7] - a specific method for self-assessment of said risk, ensuring a consistent application throughout all the entities of the Group;
- identifies and appoints a **Money Laundering Manager**[8], who acts as a **Group Representative for the Reporting of Suspicious Operations** pursuant to Art. 35 of the Italian Legislative Decree 231/2007;

7 Following the performance of the first Risk Assessment of the country's exposure to money laundering and financing of terrorism activities by the Financial Security Committee, required by the FATF of all member countries, the Bank of Italy with its communication of October 2015 required banks and banking groups to carry out a similar self-assessment exercise designed to identify the inherent risk, analyse vulnerable areas and establish the residual risk in order to implement or integrate appropriate procedures, instruments and controls to ensure the supervision of risk. This obligation was later formalised also in the primary legislation, with the promulgation of Italian Legislative Decree 90/2017 that ordered the sector Supervisory Authorities to dictate criteria and methodologies for the obligated subjects to analyse and assess the risks of money laundering and terrorism financing to which they are exposed when performing their activity. On 26 March 2019 the Bank of Italy therefore adopted the previously mentioned *"Measures regarding organisation, procedures and internal controls aimed at preventing the use of intermediaries for money laundering and terrorism financing purposes"* with the goal of regulating the effectively implemented operating procedures of the legislative provisions with its own measure.

8 See § 9.7 Group Appointee in charge of suspicious transaction reporting.

- **distributes this Policy** to all Bank entities, so that they are fully aware of risk management model that applies to anti-money laundering and financing of terrorism in compliance with the national and international regulations of reference and sector best practices;
- guarantees that the **subsidiary companies** owned by the Group shall adopt **similar policies** providing supervision and management of the risk of money laundering and financing terrorism;
- has, also using special information tools (Anti-Money Laundering Portal) and risk indicators (KRIs), an **internal controls system** regarding anti-money laundering and fighting terrorism financing aimed at monitoring activities and at tracking fulfilments set out in the model for managing these risks.

3 MANAGING THE RISK OF MONEY LAUNDERING AND TERRORISM FINANCING IN THE BANCO DESIO GROUP

3.1 Risk-based approach

With the introduction of the Fourth Anti-Money Laundering Directive, the Group is called upon to upgrade its system of monitoring systems from a rule-based approach to a risk-based approach that applies the regulatory provisions in a way consistent with its organisation and business model and in line with effectively determined risks. In compliance with these provisions, the Bank implements both the obligations provided for by legislation and its own policies in such a way as to actually adapt the measures adopted for the risk of money laundering or of terrorism financing associated with each customer / transactions based on the principle of proportionality and through a full and substantial knowledge of its customers.

3.2 Substantial knowledge of customers

In the exercise of its activities, the Bank has reconfirmed its business focus on retail Customers and the small and medium enterprises in the territory.

In consideration of that policy, the current Italian and EU regulations and the traditionally prudential approach that the Bank has always adopted, all the Bank's personnel – in accordance with the roles performed and the tasks assigned – must implement the necessary activities and cautions and ensure a proven Customer Due Diligence, in order to ensure that the overall wealth of information stored for each customer is regularly maintained and updated.

In this context the personnel must inform the customers of the obligations imposed by the anti-money laundering regulations, what they intend to achieve and the confidentiality with which the Bank may use the collected information; this makes the identification procedure much easier, as well as obtaining clarifications, further information or the required documentation backing the fulfilment required by the Customer Due Diligence.

The Group applies direct identification to customer presence as its routine procedure. The remaining methods of identification without the physical presence of the customer are to be considered exceptional, even if allowed by the Anti-Money Laundering Decree. Special attention must be paid when monitoring accounts / products operated without direct contact with the Branch or through electronic / evolved channels.

The correct registry identification is just a first aspect of Customer Due Diligence; this detail must always be accompanied by the acquisition of thorough and truthful information on the customer's economic and financial status, as well as the economic motivations behind the operations requested or performed and the purpose of the financial relationship they wish to set up. The customer’s reticence to provide accurate and updated information on their work and economic situation and assets, on the historical origin of their assets or funds channelled are to be considered elements of greater risk and of potential anomaly.

The account managers, and more in general all network personnel, help to keep customer information updated on a continuous basis – in accordance with their assigned roles -, thus implementing a constant monitoring of accounts.

To this end they integrate the customer's information file, with information they possess or news available on the streets or through reliable and independent sources to assess the coherence and compatibility of the operations undertaken with the customer's economic and financial profile, established by acquiring even data on income and assets backed by appropriate documents. All this to ensure that:

- the performance of effective due diligence on all accounts opened. In this context, special attention must be paid to subjects whose assets or sources of income come from activities considered more at risk pursuant to this Policy or for which opening accounts is not allowed;
- the acquisition and assessment of information on the purpose and nature of the ongoing relationship, checking the compatibility of the data and information provided by the customer when the relationship is started or the renewal of the due diligence using the information autonomously acquired by the bank, also regarding the total sum of the transactions made based on the aspect of other accounts previously held and the opening of additional accounts;
- the constant supervision during the on-going relationship, analysing the transactions made during the entire duration of the relationship in order to verify their compatibility and coherence with the knowledge the Bank has on its customer, its commercial activities, its risk profile, taking particular care to assess the origin and the use of the funds.

The customer "due diligence" obligations are organised into further and different levels of due diligence in proportion to the risk profile of the customer, carrying out a simplified, ordinary or enhanced due diligence as brought forward in this document and described in the Consolidated Anti-Money Laundering Law in force.

The Bank is in any way required to acquire updated information on their customers, on a minimum regular basis depending on the level of risk.

3.3 Risk-based customer profiling

The information controls that the Bank has made available to its operators will allow them to give - on the basis of processing the data and information acquired when consulting the data register, opening an account, executing occasional transactions and monitoring the transactions in place - a "rating" that represents the level of money laundering risk.

To this end, the Bank defined four levels of risk that a customer can be classified under:

Risk level	Gianos rating range
Irrelevant	1 - 5
Low	6 - 12
Medium	13 - 24
High	25 - 99

The Bank uses the Gianos Know Your customer program (hereinafter KYC) to assign an initial risk rating when opening the account / carrying out an occasional transaction; the "Risk profile management" form is used to continuously monitor the customers, allowing the above-mentioned initial rating to be raised / lowered in accordance with the transactions carried out by the customer.

The customers for whom simplified Due Diligence measures are applied when opening accounts are classified in the "Irrelevant" bracket, unless a higher risk is found.

If the customer is common to multiple Group entities, the profiling is performed by the single companies, also based on the information used by the other Group entities. Automatic mechanisms for propagating the higher risk found amongst the different Group entities are enabled.

In accordance with the Anti-Money Laundering Decree, the Bank fulfils its due diligence obligations by providing for a proportional range of activities to carry out both when the account is being opened, and during the subsequent continuous monitoring, making it proportional to the risk rating given to each customer.

More specifically, upon opening an account / carrying out occasional transactions, for "Medium" or "High" risk ratings, the Bank defined:

- a specific authorisation workflow.

- a set of further documentation / information to acquire to complete the due diligence that is tracked using a special dedicated Section in the Anti-Money Laundering Portal for the "High" bracket customers.

If there are no further risk elements, the Bank defined the following time drivers to update the information acquired, submitting the due diligence questionnaire once again to the customers:

Risk level	Time drivers for updating the Know Your customer questionnaire
Irrelevant	48 months
Low	36 months
Medium	24 months
High	12 months

Please refer to the GIANOS procedure governance tables for a description of the criteria adopted by the Bank to determine the rating; this forms an integral part of this Policy[9].

4 CUSTOMER DUE DILIGENCE GUIDELINES

The model to assess the money laundering and terrorism financing risk adopted is defined on the basis of the type of customer and the activities carried out by each Bank entity. The due diligence obligations are therefore fulfilled by making the associated risk proportional to the type of customer, "account", transaction, product or transactions in question.

The customer due diligence obligations involve the following steps:

a) identifying the customer, any representative, and checking the identity on the basis of documents, data or information obtained from a reliable, independent source;
b) identifying the "beneficial owner" of the account or the transaction and checking the identity;
c) obtaining information on the scope and nature of the account;
d) constant controls carried out while the account is in place.

The customer due diligence obligations apply to all new customers and subject to assessment of the risk, to previously acquired customers.

The Bank fulfils these obligations in accordance with the following:

- the identification and checking the identity of the customer, any representative and the beneficial owner will be carried out in the presence of the representative using a valid identification document. If the customer is a company or an entity, the actual existence of the power of representation of the representative must be checked, and information acquired to identify and check the identity of the representatives authorised to sign for the transaction to be carried out;
- the identification and checking of the identity of the beneficial owner will be carried out when the customer is being identified. The identification of the beneficial owner and the piecing together of the ownership and control structure of the legal entity can take place even without his/her physical presence on the basis of the identification data provided by the customer, or in another way, for example by consulting public registers, lists or accessible public records or documents.

9 See: (i) Items to calculate the risk profile rating from the Due Diligence Questionnaire (update of the Bank of Italy Measure of 3 April 2013); (ii) Items to calculate the risk profile rating from the Due Diligence Questionnaire (update of the Bank of Italy Measure of 3 April 2013); (iii) Links to calculate the risk profile rating from the COMMA/GIANOS procedure.

- the acquisition and assessment of information on the purpose and nature of the ongoing relationship is carried out checking the compatibility and consistency of the data and information provided by the customer using the information autonomously acquired by the bank, while also taking into account, among other things, the overall transactions during the course of the relationship;
- while the account is open, it will be constantly checked by analysing the transactions concluded during the entire duration of the relationship to ensure that said transactions are compatible with knowledge about the customer, its business activities and risk profile, having regard, if necessary, to the origin of the funds and keeping the documents, data or information up to date.

All entities belonging to the Group shall fully implement all regulatory requirements in relation to identification of the beneficial owner of accounts and, where foreseen, of operations; more specifically, the beneficial owner of customers other than natural persons coincides with the natural person or persons who, ultimately, is attributable to the direct or indirect ownership of the entity or the relevant control.

If the customer is a corporation:

a) a shareholding greater than 25 percent of the customer's capital held by a natural person constitutes specification of direct ownership;

b) a shareholding greater than 25 percent of the customer's capital held through subsidiary companies, trusts or third parties constitutes specification of indirect ownership.

Should examination of the ownership structure not allow the natural person or persons to whom the direct ownership or indirect ownership of the entity to be univocally identified, the beneficial owner coincides with the natural person or persons to whom its control is ultimately attributable on the strength of:

a) the control of the majority of votes that can be exercised at the ordinary shareholders' meeting;

b) the control of votes sufficient to exercise a dominating influence at the ordinary shareholders' meeting;

c) the existence of particular contractual obligations the allow a dominating influence to be exercised.

Should application of the criteria set out in the forgoing not allow one or more beneficial owners to be unequivocally identified, the beneficial owner coincides with the natural person or persons that hold powers of administration or management of the company.

The Bank applies the same criteria, as far as they are compatible, in the case of partnerships and of other public or private juridical subjects, even if devoid of legal personality.

In the cases in which the customer is a private juridical person pursuant to Italian Presidential Decree No. 361 of 10 February 2000, the following are cumulatively identified as being beneficial owners:

a) the founders, if alive;
b) the beneficiaries, when identified or are easily identifiable;
c) holders of management and administration functions.

In the case of a trust, the bank identifies the following as beneficial owners, in line with the provisions of Art. 22, paragraph 5 of the Anti-Money Laundering Decree:

a) the founder/settlor;
b) the trustees, i.e. the natural persons to whom management of the trust is ascribable;
c) the protectors, if they exist;
d) the beneficiaries or class of beneficiaries;
e) the other natural persons that ultimately exercise control over the assets transferred to the trust through direct or indirect ownership, or through other means;
f) any other natural person that ultimately exercises control over the trust through direct or indirect ownership, or through other means;

In the case of legal entities whose direct or indirect ownership of more than 25 percent of the share capital is attributable to a trust, the Bank - because of the higher risk related to the opacity of the chain of control - identifies all natural persons granting a trust mandate as the beneficial owners, regardless of the percentage of share that each one holds. The Bank intends to acquire the information on those granting a trust mandate also for control shares less than 25 percent of the share capital in the case of higher risk customers or of equity investments held by Trusts not registered in the separate section of Register 106 under the Consolidated Banking Law.

In identifying the beneficial owner, the following information is gathered:

- supplied in writing by the customer, under its own responsibility;
- found on public registers, lists, acts or documents in the public domain;
- obtained by other means.

As regards the legal entities entered in the Business Register of account holders, the Group has a special IT procedure aimed at checking data, during their continuous updating, with reference to the beneficial owners that can be identified based on the regulatory principle of direct and indirect ownership and of the representatives / holders of powers of representation as provided by Chamber of Commerce sources.

The information is constantly updated by the managers and by the entire Network, with the records taken from the monitoring of the customers or with information collected from reliable sources, which can form elements useful for understanding the actual ownership and control structure of the legal entity and of its latest beneficiaries.

Consistent with the forgoing, the Bank adopts the following policies / precautions in observance of the risk-based approach and principle of proportionality.

4.1 Accounts that must not be opened

In line with legislation in force, the Bank:

- will not enter into any relations, open any accounts or carry out transactions with shell banks who do not have a tax presence in the country where they are incorporated and authorised to exercise their businesses[10];
- will not enter into any relations, carry out transactions or keep already existing ongoing relations with entities other than a natural person that are directly or indirectly party[11], trust companies, trusts, anonymous companies or subsidiaries through bearer shares having offices in a third high risk country[12]
- shall not set up relations or carry out transactions when it is not possible to establish the certain identity of the Beneficial Owner, especially as regards customers having offices in a third high risk country[13]
- shall not, in any form, open accounts or savings books in anonymous form or with fictitious registration[14];
- if the adequate customer verification activities are transferred to third parties, shall not make use of third parties located in a third high risk country[15];
- will not set up relations with subjects that have not completed a due diligence process Therefore, the Bank is required to acquire updated information on their customers, on a regular basis depending on the level of risk.

In addition to the cases mentioned, also in consideration of autonomous corporate evaluations based on the low risk appetite and on the business model identified, and in line with the “risk-based approach” principle, the Bank:

- no accounts will be opened with natural persons if the customer claims that the beneficial owner is a third party or in all instances in which it transpires that the account has been set up “through an intermediary”;

10 See Italian Legislative Decree 231/2007, Art. 25, paragraph 3.

11 Regardless of the shareholding and level at which it is placed.

12 See Italian Legislative Decree 231/2007, Art. 42, paragraph 2.

13 See Italian Legislative Decree 231/2007, Art. 42, paragraph 2.

14 See Italian Legislative Decree 231/2007, Art. 50, paragraph 1.

15 See Italian Legislative Decree 231/2007, Art. 29, paragraph 1.

- will not set up continuous direct relations with foreign trust funds, regardless of where they are established, or national trust funds that are not registered in the separate registry 106 TUB[16] and applies the stronger due diligence measures when setting up relations with trust funds registered in the separate Registry 106 TUB. It is also forbidden to open so called "Omnibus" accounts in the name of trust companies even if registered and/or to financial brokers. Any exceptions must be submitted to the General Manager for authorisation;
- does not offer the correspondent accounts with foreign banks service, regardless of the country where established;
- will not open accounts/carry out transactions with the following category of subjects:
  a) parties on the national or international black lists (UN, OFAC, EU)[17];
  b) Names that act in their capacity as electoral agents to gather funds to be used to finance electoral campaigns[18];
  c) parties that produce arms (including so called "dual use" assets and technologies which may be used for civil purposes but also in the production, development and deployment of military armaments, as regulated by the sector regulations[19]), ammunition or weapons of mass destruction;
  d) parties that manage casinos and gambling houses, licensees and distributors of games or videolotteries (VLT) online or on a physical network[20];
  e) parties that solely or mostly manage a gaming business[21];
  f) money transfers[22] and money exchange;
  g) credit recovery agencies[23];
  h) parties that solely or mostly manage a gold buying business or professional gold operators[24];
  i) suppliers of virtual currency utilisation services[25];
  j) securitisation transaction vehicle companies;
  k) parties that produce and/or market so-called legal cannabis (Light Cannabis Sativa) [26]

4.2 Reinforced due diligence measures

In compliance with the regulatory provisions in force and taking into account the guidelines issued by the European Supervisory Authorities on risk factors, and on the basis if autonomous assessments based on its organisation and business model and on a low risk appetite, the Bank adopts the following measures to strengthen its monitoring of money laundering and terrorism financing risks:

16 Art. 199 of the Consolidated Law on Finance, as modified by Italian Legislative Decree 141/2010 requires that trusts directly or indirectly controlled by a bank or a financial broker, or that have adopted the form of a public company and have fully paid up share capital not below 100,000 euro, must request authorisation from the Bank of Italy in order to be registered in the separate section of the Register pursuant to art. 106 TUB. Once the foreseen transitional regime closed, on 12.5.2016, the Bank of Italy Circular no. 288 of 15 April 2015 became fully effective and the trust funds registered in the 106 TUB Registry are subjected to the direct supervision of the Bank of Italy even in relation to the dispositions on combating money laundering contained in Italian Legislative Decree 231/2007.

17 These lists are constantly updated by World Check.

18 See Law 515 of 10 December 1993.

19 See Law No. 185 of 9 July 1990 and its subsequent amendments.

20 See Italian Legislative Decree 231/2007, Art. 1, paragraph 3, letters c) and f) and Art. 3, paragraph 6, letter c).

21 See Italian Legislative Decree 231/2007, Art. 3, paragraph 6 letters a) and b).

22 *Cfr*. Italian Legislative Decree 11/2010, Art. 1, paragraph 1, letter b), number 6).

23 *Cfr*. article 115 TULPS (Consolidated Act on Public Security).

24 See Italian Legislative Decree no. 92 of 25 May 2017 and Italian Law No. 7 of 17 January 2000, respectively.

25 See Italian LegislativeDecree 231/2007, Art. 1, paragraph 2, letter ff), Financial Information Unit Communication of 30 January 2015 and of 28 May 2019"Anomalous use of Virtual Currency"; and Bank of Italy "Virtual Currencies - Communications to the system".

26 Cultivation and agro-industrial supply chain of cannabis with low active ingredient regulated by Italian Law No. 242 of 2 December 2016.

- Diversified internal authorisation processes by means of specific procedural workflows, based on the customer risk profile[27]; more precisely:
  - authorisation from the Anti-Money Laundering Office when opening accounts for parties with a "high" risk profile;
  - assessment by the Branch Manager and authorisation to the printing of the Customer due diligence Renewal Questionnaire for customers in the "high" risk bracket;
- In a specific section of the Anti-Money Laundering Porta, tracking: (i) of the assessments of the Branch Manager regarding exposure to the risks of money laundering and terrorism financing of customers classified in the "high" risk bracket, carried out during constant monitoring (maintenance of existing accounts) or when setting up new accounts; (ii) of adequate and pertinent supporting documentation.
- Application of enhanced due diligence measures regardless of the risk profile given by the computer procedures in the following cases:

a) opening of accounts for customers that are not present (operating remotely);
b) correspondent accounts with corresponding entities in non-EU countries28;
c) where there are cash or security deposits made from other countries;
d) if a report on a suspicious transaction is sent to the Financial Information Unit;
e) in relation to using products, transactions or technology that could increase the risk of money laundering and/or the financing of terrorism (for example favouring anonymity);
f) when dealing with high value banknotes29;
g) in the case of transactions distinguished by unusually high amounts or with regard to which there are doubts on the purposes for which they are actually arranged;
h) to natural persons holding, or have ceased to hold for less than one year, important public offices (politically exposed persons - PEPs), as well as their family members and those who notoriously have close ties according to the definitions of Italian Legislative Decree 90/2017. According to the risk-based approach, the Bank applies the following additional criteria:
   - inclusion of brothers/sisters in the notion of "family members" of PEPs
   - registration of the Cardinals of the Catholic Church, or of Bishops and Archbishops if they hold bishop's sees,30 and University Chancellors
   - extension of the status of PEP also to additional offices held at the large Local Administrative Body level (Provinces, Local Joint Municipal Unions, Free Consortia of Municipalities) as specified in the table shown below.

   To ensure verification of whether customers belong to the aforementioned categories, the Bank has implemented procedures that use specific lists made available and updated by external info providers (World Check) or other similar source with an appropriate level of reliability and that cause automatic risk rating increase and propagation mechanisms;

27 For a more thorough description of the risk classes please refer to paragraph § 4.2.

28 Service currently not offered by the Banco Desio Group.

29 The Bank does not circulate high value banknotes (€ 200 and 500).

30 Emeritus bishops or holders of honorific/administrative offices are excluded.

	ORDINARY STATUTE REGIONS				SPECIAL STATUTE REGIONS	
	REGION	**METROPOLITAN CITY**	**PROVINCE**	**MUNICIPALITY**	**PROVINCE**	
PEP	- President - Vice President - Councillor - President of the Reg. Council - Vice President of the Reg. Council - Reg. Councillor	- Mayor - Deputy Mayor	- President - Vice President - President of the Prov. Council - Mayor of the Prov. Capital	- Mayor of Municipality with residents = > 15,000 - President of the Mun. Council with residents = > 15,000	- President of the Prov. Council - Vice President of the Municipal Council. - President of LJMU/FCM - Mayor of the Prov. Capital	=

i) the opening of accounts referring to political parties is subject to the authorisation of the General Manager;

j) parties involved in criminal investigations or proceedings, identified in records processed by the Database used to manage investigations by the public prosecution service and reported to the Bank or through access to open sources;

k) customers that belong to the "High" risk bracket pursuant to the profiling carried out through the applications in use;

- In consideration of the geographical risk, the Bank applies:

a) operational blocks on transactions with counterparties located in countries under embargo or with restrictions imposed by International Organisations as regards the export of weapons and "dual use" goods; embargo on nuclear and mass destruction weapons and the freezing of assets of natural persons and/or other entities31;

b) reinforced due diligence measures in the case of accounts open to non-residents with specific regard to those relating to parties resident in countries considered "non cooperative/with gaps in the money laundering and terrorism financing risk systems"32 or under embargo or with restrictions imposed by International Organisations;

c) reinforced due diligence measures in the case of transactions with counterparties located in black listed tax haven countries33 or included in the Countries described under points b) and d);

d) particular precautions taken against transactions from/to countries with a high corruption risk34 or considered by the Group at increased risk35 due to the presence of factors that determine a higher risk of money laundering/self-laundering - terrorism financing.

The Parent Company periodically monitors the classification of the Countries based on the type of associated risk while taking into account - among other things - risk mitigation factors (e.g. presence of tax information exchange agreements[36]) and updates at lease once a year the list of Countries forming an integral part of this Policy.

4.3 Enhanced due diligence measures

In line with its organisation and business model and taking into account the low risk appetite, the Bank:

- Provides for diversified internal authorisation processes by means of specific procedural workflows, based on the customer risk profile; more precisely:

  - authorisation from the Branch Manager when opening accounts with parties having "medium" risk profiles;
  - assessment by the Branch Manager and authorisation to the printing of the Customer due diligence Renewal Questionnaire for customers in the "medium" risk bracket;

31 See List of Countries published on the Anti-Money Laundering Portal - "COUNTRIES UNDER EMBARGO / RESTRICTIONS".

32 As identified by FATF in international fora – See http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/ and by the European Commission - See List of Countries published on the Anti-Money Laundering Portal - "*EU AND FATF – CRITICAL ISSUES IN COOPERATION/GAPS IN THE ANTI-MONEY LAUNDERING AND TERRORISM FINANCING SYSTEMS*".

33 See List of Countries published in the Anti-Money Laundering Portal - "ECOFIN – NON-COOPERATIVE TAX JURISDICTIONS" and "CONSOLIDATED TAX ACT - TAX HAVENS".

34 See List of Countries published on the Anti-Money Laundering Portal - "TRANSPARENCY INTERNATIONAL - CORRUPTION RISK".

35 See List of Countries published on the Anti-Money Laundering Portal - "BANCO DESIO GROUP - INCREASED RISK".

36 See List of Countries published on the Anti-Money Laundering Portal - "MEF (MINISTRY OF ECONOMY AND FINANCE) - AUTOMATIC EXCHANGE OF INFORMATION".

- assessment of the Anti-Money Laundering Office/Foreign Area for opening current accounts to "non resident" subjects, regardless of the risk bracket.

- Believes in general that the trust interpositions, similar screens regarding the beneficial ownership of legal entities, the extreme complexity of the control chain or the reluctance to provide information on the end financial beneficiary form an increased risk factor. As a result, in relations with "third parties" and customers whose company's shares are held through a trust, it shall acquire from the latter a specific certification regarding the identity of the actual beneficiary or of the screened subjects that hold the shares. In these cases, self-certifications provided by the customer are not allowed.

- Regardless of the profile assigned to the customer by the established procedures, an enhanced risk will always be assigned to accounts opened on behalf of:

a) Non-profit organisations;
b) Trust;
c) Foundations;
d) Subjects that have business with the Public Administration, given the possibly corruption risk;
e) Trusts or legal entities in which trusts have an interest;
f) Legal entities with non-transparent control structures;
g) Customers managed through private bankers or through financial consultants.

Ranking increases are contemplated for these categories of subjects, or specific records are provided in the Anti-Money Laundering Portal, in order to simplify its constant monitoring by the Branch Manager.

h) Italian Local Politicians ILP), as can be found in the Register of Local Administrators published on the website of the Italian Ministry of the Interior (http://amministratori.interno.it/), not included on the list of politicians described above, under letter b) and as specified n the table provided below and for which automatic risk ranking increase mechanisms are provided;

	ORDINARY STATUTE REGIONS				SPECIAL STATUTE REGIONS	
	REGION	METROPOLITAN CITY	PROVINCE	MUNICIPALITY	PROVINCE	
ILP	=	- Metropolitan Councillor	- Provincial Councillor	- Mayor of Municipality with residents < 15,000 - Deputy Mayor - Municipal Councillor	- Municipal Councillor	- Provincial Councillor

i) Subjects that operate in waste disposal, health, renewable energies, owing the risk of infiltration by organised crime;
j) Subjects that carry out their activities in the following sectors: cleaning and maintenance; consultancy and advertising, iron metals, construction, haulage and earth moving, precious metals, artworks, cosmetics market, wholesalers of oil and grains, exchange of services and negotiated rights on IT platforms, sale of cars and car accessories, products with a high technological content (computers, mobile phones), which – according to the findings of the UIF – have a greater tendency to be exposed to instances of fraud and false invoicing;
k) Subjects involved in operations connected with the dispensing and use of EU and national public funds that - according to the findings of the UIF - are more subject to the risk of corruption or abuse in dispensation and management of public funds.

The increased measures entail the Branch Manager / Account Manager to perform a more meticulous assessment regarding setting up accounts with the aforementioned categories of subjects, the acquisition of a more extensive wealth of documented information, and a critical and in-depth analysis of the overall consistency / compatibility of the operations undertaken compared to what has been proposed / is expected, supported by appropriate documentation.

These measures must be adopted in all situations in which the characteristics of the customer, of the transaction or of the ongoing relationship objectively represent a higher risk compared to the ordinary risk, regardless of the risk rating given by the procedures and of the inclusion in specific categories.

4.4 Simplified due diligence measures

When there is a low risk of money laundering and terrorism financing, to be recorded based on specific factors, such as the business or profession carried out by the customer and by their beneficiary owner; the reputation of the customer and of their beneficial owner or the nature and conduct of the customer and of their beneficial owner, the Bank takes simplified due diligence measures in terms of the extension and frequency of the required obligations.

Based on the regulatory provisions issued up until now or under consultation and the joint guidelines of the European Supervisory Authorities, it is possible to identify and establish the following measures by way of example:

- modulating the time for executing activities to identify the customer or the beneficial owner, by postponing acquisition of the copy of the ID document up to thirty days;
- checking the identity of the beneficial owner by solely acquiring a statement confirming the data signed by the customer under their responsibility;
- using assumptions in identifying the purpose and nature of the ongoing relationship in connection with products designed for a specific use;
- reviewing the customer's risk profile when specific circumstances arise (such as the opening of a new type of account), and in any case at least every five years;
- reducing the frequency and depth of the controls carried out when monitoring the account.

In line with the forgoing, the Bank takes into consideration - among other things - the following low risk indices:

a) risk indices relating to customer types such as:
   - companies admitted to listing on a regulated market and subject to disclosure obligations imposing the obligation to ensure adequate transparency of the beneficial ownership;
   - public administrations or institutions or organisms that perform public functions, in compliance with European Union law;
   - customers residing in low risk geographical areas, pursuant to letter c) below;

b) risk indices relating to types of products, services, transactions or distribution channels such as (by way of example):
   - life insurance contracts falling within the segments listed in Art. 2, paragraph 1 of the CAP in the case that the annual premium does not exceed Euro 1,000 or whose single premium is of an amount no higher than Euro 2,500;
   - forms of supplementary pension regulated by Italian Legislative Decree no. 252 of 5 December 2005, provided that they do not contain payment clauses other than those contained in Art. 14 of the same decree and that cannot be used as guarantee for a loan outside of the cases provided for by law;
   - social security or similar systems that pay pension benefits to employees, whose contributions are paid by detracting from the remuneration and that do not allow the beneficiaries to transfer their rights;
   - financial products or services that offer appropriately defined services limited to certain types of customers, aimed at promoting financial inclusion;
   - products whose risks of money laundering or terrorism financing are mitigated by factors such as expenditure limits or transparency of the ownership;

c) risk indices regarding geographical areas such as:
   - Member states of the European Union;
   - Third countries that have effective money laundering and terrorism financing prevention systems;
   - Third countries that authoritative and independent sources appraise as being marked by a low level of corruption or of permeability to other criminal activities;

- Third countries that based on reliable and independent sources, such as mutual assessments or published detailed assessment reports, provide for and actually apply money laundering and terrorism financial prevention measures consistent with the FATF recommendations.

When issuing the customer due diligence Provisions[37], in order to initially tangibly apply simplified customer due diligence measures and without prejudice to the obligation to adapt its extension to the risk actually recorded, the bank:

- has introduced some implementations to the IT procedures that allow fulfilment of the customer due diligence obligations to be managed, also in the cases in which the presence of a low risk is revealed. In these cases, the ID data of the beneficial owner and a specific due diligence questionnaire simplified in its contents are always acquired for newly opened accounts;

- takes simplified due diligence measures only as regards the following types of customer/account:

  a) Public Administration, as defined in the Anti-Money Laundering Decree[38];

  b) Bank and financial intermediaries listed below[39]:
     - banks;
     - Poste italiane S.p.a.;
     - electronic money institutions as defined by Art. 1, paragraph 2, letter h-bis), Consolidated Banking Law (IMEL);
     - payment institutions as defined by Art. 1, paragraph 2, letter h-sexies), Consolidated Banking Law (IP);
     - investment firms as defined by Art. 1, paragraph 1, letter e), Consolidated Law on Finance (SIM);
     - asset management companies as defined by Art. 1, paragraph 1, letter o), Consolidated Law on Finance (SGR);
     - open-end investment companies as defined by Art. 1, paragraph 1, letter i), Consolidated Law on Finance (SICAV);
     - capital assets investment companies as defined by Art. 1, paragraph 1, letter i-bis), Consolidated Law on Finance (SICAF);
     - intermediaries entered in the register provided for by Art. 106 of the Consolidated Banking Law, except for credit guarantee consortia;
     - Cassa depositi e prestiti S.p.a.;
     - insurance companies operating in the segments listed under Art. 2, paragraph 1, CAP (Private Insurance Companies Code);
     - branches of bank and financial intermediaries and of insurance companies having registered office and central administration in another member state or in a third state not included in those considered at higher risk by the Bank.

  c) Accounts registered to Bankruptcy/Executive Procedures listed below[40]:
     - Bankruptcies;
     - Composition with creditors;
     - Compulsory administrative liquidations;
     - Executive Procedures.

- check the continuation of a low risk of money laundering over time with the aim of understanding whether the customer might continue to benefit from application of simplified due diligence measures. Specifically, the Bank

37 Bank of Italy placed the aforementioned Provisions under public consultation in April 2018.

38 See Art. 1 - Paragraph 2 - Letter hh). An exception is made for the following categories, subjected to ordinary due diligence:
- PA investee companies and their subsidiaries pursuant to Art. 2359 of the Italian Civil Code;
- schools and private and/or state-recognised schools of all kinds and levels;
- universities, both public and private;
- State companies and administration with autonomous systems;
- chambers of commerce, industry, handicrafts and agriculture and their associations.

39 In so far as they are recipients of the anti-money laundering obligations and subject to the sector Supervisory Authorities.

40 In so far as they are opened as instructed by the Court, are managed by receivers / commissioners appointed by the Judicial Authority, with limited operations previously authorised by the same judicial authority.

refrains from applying the simplified measures and meets the ordinary or strengthened due diligence obligations in the cases in which:

- the conditions for applying the simplified measures cease to exist based on the risk indices provided for by the Anti-Money Laundering Decree and by this Policy;
- the monitoring of all of the customer's operations and the information acquired during the relationship lead one to exclude the presence of a low risk profile;
- there is, in any case, a suspicion of money laundering or terrorism financing.

5 GUIDELINES ON MONITORING THE RISK OF TERRORISM FINANCING AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

Taking into consideration the significant threat arising from international terrorism and from the proliferation of weapons of mass destruction, the Bank places primary importance on actions to fight these phenomena, to be implemented both when relationships start up and during the monitoring of the financial transactions. To this end:

- the Bank, with the support of the IT Outsourcer and – through said outsourcer – other external InfoProviders, adopts internal procedures designed to prevent the setting up of banking relations or the performance of operations by subjects found on the international black lists and constantly verifies that they are updated and effective;
- monitors the payments made / received from the customers regarding any presence of the counterparties on the international black lists using the above procedures;
- using special procedural blocks and with application of strengthened due diligence measures, checks the transactions from/to abroad with counterparties located in high risk Countries or with particular shortcomings. Special attention is paid to applying restrictions set for the Countries under embargo or for the transactions regarding nuclear and mass destruction weapons, military technologies and Dual Use goods;
- verifies the implementation of appropriate money laundering and terrorism financing risk monitoring by banking counterparties with which correspondence accounts/relations have been set up or SWIFT key exchanges are enabled, paying attention also to the geographical and reputation risk of the counterparty;
- monitors the issue of the fight against arms proliferation even by including in the procedure special case lists that will trigger blocks.

6 INFORMATION FILING GUIDELINES

The Bank is aware of the importance of thoroughly meeting the obligations of filing documents, data and information acquired during due diligence; the purpose is to prevent, identify or reconstruct, in retrospect, the commission of money laundering or terrorism financing activities, if any, and to allow investigations and analyses to be conducted both in-house and by the competent authorities. To this end the Bank:

- has set up and uses the Central Computer Archive as a standardised archive and chief tool for meeting the obligations of filing data and information concerning the operations of its customers, supervising its proper feed continuously with the support of the IT Outsourcer and the Organisation and Systems Area;
- it also avails itself of the information on sector archives and dedicated data bases containing data and additional information referring to the transactions performed by its customers and to the accounts they hold with the Bank;
- with the support of the IT Outsourcer, guarantees that the data recorded in the Central Computer Archive are aggregated using IT procedures and are periodically sent to the Financial Information Unit according to the standards, the methods and the time frame established by the same Authority;
- processes the data and information in the Central Computer Archive in compliance with personal data protection rules and guarantees:

- complete and prompt accessibility to the data and information by the Authorities and entitled subjects (e.g. in the cases customer due diligence obligations are executed by third parties);
- the acquisition of documents, data and information, with the relevant date indicated, within 30 days from when the account is set up, from execution of the transaction, from the change and closing of the account;
- the integrity of the data and information, and their non-alterability after they are acquired;
- the transparency, completeness and clearness of the data and information as well as maintenance of data history.

7 ACTIVE COLLABORATION AND REPORTING OF SUSPICIOUS TRANSACTIONS GUIDELINES

The personnel of the Bank and Group is fully aware that active collaboration in fighting money laundering and terrorism financing phenomena is not merely to meet specific regulatory obligations, but that it instead has ethical value and plays a particularly important role for the effectiveness of the overall risk prevention system, also reputation in nature.

All employees are therefore required to:

- become familiar with the internal and external regulatory provisions on reporting suspicious transactions, the anomaly and behavioural indices circulated by the competent Authorities, and the procedures to adopt to set the reporting procedure in motion, while keeping their knowledge and skills to this regard up to date;
- promptly implement the obligations of reporting suspicious transactions recording during customer substantial due diligence, the constant monitoring of the accounts and - more in general - during any activity concretely executed in connection with the assigned duties;
- supervise compliance of all employees with the suspicious transaction reporting provisions and - more in general - with the rules and procedures adopted in order to prevent money laundering and terrorism financing, by promptly reporting any potential or actual breaches following the whistleblowing procedures the Bank has in place.
- comply with the rule of not notifying the customer concerned or third parties of the report made, of the sending of additional information requested by the Financial Information Unit or of the existence or probability of investigations or in-depth analyses on the subject of money laundering or financing terrorism.

In order to tangibly implement the active collaboration obligations, the Bank:

- has a special IT application for reporting suspicious transactions that is accessible to all employees and such as to ensure the appropriate tracking of the SOSs and protection of the confidentiality of the reporting parties. It has also defined internal procedures to follow for forwarding reports. Among other things, these procedures include:
  - a process for assessing suspicious transactions based on a dual level: Manager / Head of the Secondary Unit, Branch, Hub or Spoke, or of the Head Office (first level) and Group representative (second level), with the possibility for each employee to forward an SOS also directly to the Group representative;
  - the right for the Group representative to make autonomous reports to the Financial Information Unit, regardless of the receipt of a first level SOS;
  - the obligation to give the first level a feedback on the forwarded reports containing information on the management of the customers / accounts the SOS concerns and - in the case of reports not forwarded to the Financial Information Unit - the reasons the led to the filing of the reports considered groundless;
  - the return to the reporting Branch / Operating Unit of any feedback received from the Financial Information Unit on the reports that proved to not contain sufficient elements of suspicion;
- has IT tools that can track records of potentially anomalous / unexpected transactions that should be analysed and studied in-depth in order to assess their compatibility / consistency with the subjective profile of the customers involved. These records are periodically submitted to the scrutiny of the first level, called upon to track, in the IT applications, the decisions taken regarding whether or not there are conditions for forwarding an SOS and for arguing their assessments with the support of adequate documentation;
- widespread circulation of the procedures to be adopted to start up the reporting process and to assess a potential anomaly in the behaviours / transactions of the customers by publishing the internal regulation; periodic training

activities; making available, in the Anti-Money Laundering Portal, specific anomaly indicators drawn up by the Bank of Italy and Anti-Money Laundering Outlines and Books drawn up by the Financial Information Unit;

- also taking into consideration the Code of Ethics and the MOG 231, generally considers inconsistent with an SOS the maintenance / development of the accounts with the names involved in it and with the affiliates. When explicitly requested by the Anti-Money Laundering Function, accounts must be closed with utmost professionalism, while taking all precautions in order to safeguard the confidentiality of the report and to limit all potential legal and reputation risks, even of a simple complaint. When there are existing credit facilities, the Branch coordinates with the Functions in charge of the credit facilities in order to best protect the bank's credit rights.

8 GUIDELINES ON ANTI-MONEY LAUNDERING TRAINING AND WIDESPREAD RISK PREVENTION CULTURE

Effective application of the anti-money laundering legislation implies full knowledge of its purposes, related principles, obligations and corporate responsibilities.

The Group places primary importance on the professionalism and training of its personnel and financial consultants, on the continuous updating of skills and on the creation of a widespread culture as tools that can effectively prevent risks of money laundering and financing terrorism, as well as reputation risks. In such a context the Bank:

- provides personnel educational and training programmes on the obligations set by anti-money laundering legislation. Particular attention is paid to the specific preparation of the personnel in closer contact with the customers and the Anti-Money Laundering Function staff; the latter are required to be continuously updated on the evolution of money laundering risks and on the schemes typical of criminal financial transactions.
- the personnel educational and training activity is carried out on an ongoing and systematic basis as part of staff programmes; the Anti-Money Laundering Function:
  - sends the Human Resources Department a note containing the bank personnel training requirement every year;
  - provides specialised support and collaboration in providing training to the personnel and in educating them on the proper use of the tools and procedures being used;
  - submits a report on the educational and training activities provided on the subject of anti-money laundering to the approval of the body in charge of strategic supervision as part of the annual report.
- In compliance with the regulatory obligations and provisions of this Policy, all personnel and external collaborators (Financial Consultants and Agents) of the Group are required to follow the prepared educational and training programmes and are called upon, also through constant consultation and familiarity with the corporate rules on operations and self-training, and to have an adequate and up to date knowledge of the legislation and of the related responsibilities, and to be able to consciously use the tools and supporting procedures when carrying out their duties.

9 ORGANISATIONAL SAFEGUARD MEASURES AGAINST THE RISK OF MONEY LAUNDERING AND TERRORISM FINANCING

In accordance with the provisions of prevailing law[41], the Bank established a department - called the Anti-Money Laundering Office - which will supervise its commitment to prevent and manage the risk of involvement in anti-money laundering events and financing of terrorism.

41 *See* "Measures regarding organisation, procedures and internal controls aimed at preventing the use of intermediaries for money laundering and terrorism financing purposes" (Bank of Italy, 26 March 2019).

Given that the entire company structure will also have to be involved to effectively monitor the risks in question, priority is given to the role carried out by the company bodies, the various Departments, Offices and Operating Units, and by specific positions. The tasks they are assigned and their proper execution form the basic measure taken to mitigate the risk.

In accordance with those principles, the organisational measures taken assign clearly defined roles and responsibilities for the following parties:

- Board of Directors
- Officer in charge of the internal control and risk management system – "AISCI" (if appointed)
- Board of Statutory Auditors, also in its capacity as Supervisory Board in accordance with Legislative Decree 231/2001.
- Control and Risk Committee
- General Manager
- Anti-Money Laundering Office
- Group Appointee in charge of suspicious transaction reporting
- Person responsible for Anti-Money Laundering at each partner company that is part of the Group
- Anti-Money Laundering contact person in the Organisation and Systems Area
- Internal Audit Committee
- Risk Management Department
- Human Resources Department
- Compliance Office
- Other Business Unites

9.1 Board of Directors

The Board of Directors monitors the risk management process and by approving this Policy, defines the strategic guidelines and governance policies related to the various significant profiles on the subject of organisational structures, procedures and internal controls, and adequate checking and filing of data with regard to the risks associated with money laundering and terrorism financing to apply at Group level. In line with the provisions of the "Management of information flows" and the document "Information flows relating to the company bodies and internal control departments. Parent Bank Rules and guidelines for interaction with the Subsidiaries", the Board of Directors receives the infra-group information flows from the subsidiaries, and aimed to provide information to the Parent Bank for strategic supervision purposes that include the issue of anti-money laundering.

To that end, the anti-money laundering policy establishes a united, coordinated internal control and monitoring system and guidelines, aimed at promptly identifying and managing money laundering risk, and defines a complete and timely information flow system towards the company bodies, also in order to ensure that the strategic supervisory body is kept informed about any shortcomings/anomalies encountered.

More specifically, the Board of Directors is in charge of the following:

- approving the establishment of the Anti-Money Laundering Function by identifying its tasks and responsibilities, as well as the methods for coordinating and collaborating with the other corporate control functions;

- appointments and terminations, in accordance with the Board of Statutory Auditors and the Anti-Money Laundering Office Manager (hereinafter the "Anti-Money Laundering Manager") and the Suspicious Transaction Reporting Manager;

- defining and periodically re-examining, in line with the results of the self-assessment or when there are significant changes made to the business model, the strategic positions and risk governance policies related to money laundering and terrorism financing, ensuring the adequacy of the risk management and control system, including through assigning the applicable bodies or committees the authorisation system and duties and ensuring their effectiveness over time;

- approving the principles for managing relationships with the customers classified "high risk";

- assessing the risks ensuing from transactions with third countries associated with higher risks of money laundering and corruption, while identifying them and monitoring the effectiveness of the measures taken to mitigate them;
- continuously ensuring that the duties and responsibilities relating to anti-money laundering and combating terrorism financing are allocated clearly and appropriately, ensuring that: (i) the business and control functions are separate; (ii) the Anti-Money Laundering function is provided with sufficient and appropriate resources; (iii) the Anti-Money Laundering function is assigned an annual expense budget;
- ensuring that an adequate, complete and prompt system for passing information to the company bodies and between the control functions is prepared;
- ensuring protection of confidentiality in the procedure of reporting suspicious transactions;
- defining – consistently with the instructions provided by the Bank of Italy – the methods used when carrying out the regular self-assessment exercise on the exposure to the risk of money laundering and financing of terrorism of the Bank and Group and in assessing its results and in approving the proposed correction measures/remedy actions;
- examining, at intervals established by the Flow Monitor, the Accounts, the Dashboard and more in general every informative document produced by the Anti-Money Laundering Manager relating to the activities carried out by the Anti-Money Laundering function;
- examining, at intervals established by the Flow Monitor, the reports prepared by the control functions and, on an annual basis, the document on the results of the self-assessment of money laundering risks;
- ensuring that the shortcomings and anomalies emerging from the controls at various levels are promptly brought to its attention and promoting the adoption of appropriate corrective measures, the effectiveness of which it assesses.

9.2 Manager responsible for the risk management and control system" (AISCI)

- must ensure that an effective system of internal control and management of the risk of money laundering and financing of terrorism is constantly maintained.
- implements the strategic guidelines and the risk governance policies decided by the Board of Directors in relation to anti-Money Laundering and fighting the financing of terrorism, by overseeing the planning, implementation and management of the internal risk management and control system, constantly verifying the appropriateness and effectiveness of the system itself, as well as the initiatives and actions that may be taken to guarantee that it is always complete, appropriate, functional and reliable. He/she shall also ensure that the results of the verifications performed are brought to the attention of the Risk and Control Committee and the Board of Directors;
- supplies the General Manager with indications on the implementation of the Bank's strategic policies to combat money laundering and terrorism financing, identifying the company departments involved and bestowing on them specific responsibilities in accordance with the law and the competent authorities;
- receives all the information flows designed to ensure that all the company departments involved and the organisms responsible for control functions are aware of the risk factors, with particular attention paid to the information flows from the Anti-Money Laundering Function;
- verifies that adequate operating procedures are adopted that allow the customers to be correctly identified, the acquisition and update of information that can help define the risk profile, the identification of the financial reasons underlying the accounts opened and the transactions carried out, the timely fulfilment of communication obligations to the authorities provided by law with respect to combating money laundering and terrorism financing. More in general he/she verifies the implementation of the required corrective or updating actions when failures or anomalies are reported, or following the introduction of new products, activities, services or relevant processes;
- ensures that the internal risk management and control system, where money laundering and the fight against the financing of terrorism are concerned, is readily adapted to comply with legislative and regulatory developments as well as the dynamic of operating conditions and the management performance; the function identifies possible changes to be made to the system itself to be presented before the Board of Directors, having first received an opinion of the Control and Risk Committee and the Board of Statutory Auditors, and verifies their implementation;

- forwards to subsidiary companies – within the context of the management, coordination and control activities of the Banking Group's companies and of the other subsidiary companies – the instructions dictated by the Board of Directors relative to the system of internal control and risk management, where money laundering and the fight against the financing of terrorism are concerned, with the support of the internal control functions of the subsidiary companies (whether or not they are centralised at the parent company's offices).

9.3 Body with control duties

The **Board of Statutory Auditors** will monitor compliance with the regulations and the completeness, functional capacity and adequacy of the anti-money laundering controls. In the exercise of its duties, the body with control duties will enlist the assistance of the Anti-Money Laundering Office and the Internal Audit Committee to carry out the checks and controls necessary and use the information flows from the other company bodies, the Anti-Money Laundering Manager and the control bodies.

More specifically, the Board of Statutory Auditors, including with the support of the other control departments:

- carefully assesses the suitability of the procedures in place to carry out the customer due diligence checks, register and file the information and report suspicious transactions;
- analyses the reasons for the shortcomings, anomalies, and irregularities found, and promote the adoption of suitable corrective measures;
- supervises compliance with the rules contained in Italian Legislative Decree 231/2007;
- notifies the Group representative of potentially suspicious transactions it becomes aware of while performing its duties without delay;
- notifies, without delay, the sector supervisory authority and the administrations and bodies concerned based on their respective competences of events that might complement serious, repeated, systematic or multiple breaches of the provisions set out under Section II of Italian Legislative Decree 231/2007 and the related implementing provisions that it becomes aware of while performing its duties[42].
- it will be consulted regarding decisions concerning the appointment and the revocation of the Anti-Money Laundering Manager and of the Suspicious Transaction Reporting Manager, as well as in connection with the definition of the overall organisational elements of the management and control system against the risk of money laundering and financing terrorism.

The Board of Statutory Auditors, also in its capacity as **Supervisory Board in accordance with Legislative Decree 231/2001**, supervises the upkeep of the 231 Organisational model in relation to lending offences and offences relating to the subversion of democracy (pursuant to article 25-*quater* Legislative Decree 231/2001) and the crimes of receiving stolen goods, money laundering, the use of money, goods or benefits from illegal sources and self-laundering (pursuant to article 25-*octies*, Legislative Decree 231/2001). In the execution of its duties, the Body receives information from the company departments and can access all the relevant information without limits, in order to carry out its duties.

9.4 Control and Risk Committee

The **Control and Risk Committee** acts as consultants, make proposals and assist the Board of Directors as it ensures that the internal control system is functioning properly. To that end, the Committee will report to the Board of Directors on its activities and the adequacy of the internal control system on a regular basis. Within the scope of combating money laundering and terrorism financing, the Committee will work in association with the Anti-Money Laundering Office, and has the right to ask for more specific in-depth investigations to be carried out.

9.5 General Manager

- ensures that the procedures needed to fulfil obligations of customer due diligence and filing the documents and recording the information in the Central Computer Archive are arranged, including with respect to the computer aspects;
- ensures that instruments are adopted, including computer instruments, to identify anomalous transactions and a suspicious transaction reporting procedure that can guarantee certainty of the references, standardisation of behaviour, maximum confidentiality and the general application to the entire structure;

42 Without prejudice to the disclosure obligations set out in Art. 46 of Italian Legislative Decree 231/2007, the members of the control bodies of the obliged entities are exempt from the obligations established under Section II, paragraphs I, II and III of the Anti-Money Laundering Decree.

- adopts protective and/or disciplinary measures with respect to staff, in relation to the failure to comply with the provisions regarding combating money laundering and terrorism financing;
- approves the training and instruction programs for employees and external staff regarding the obligations resulting from anti-money laundering and international terrorism financing regulations;
- authorises the opening/maintenance of named accounts or accounts that can be traced to politically exposed persons (PEPs) or political parties/organisations connected with political parties[43] and confirms any subsequent loss of PEP status;
- provides support to the Board of Directors through the Anti-Money Laundering Function in connection with the implementation of the corrective or adaptation measures to be taken in order to prevent and mitigate the residual risk as identified by the result of the self-assessment.

9.6 Anti-Money Laundering Office

The Anti-Money Laundering Office will continuously check that company procedures reflect the aim of preventing and combating breaches of both external and internal regulations against money laundering and terrorism financing. It carries out II level controls in order to monitor said risks.

In carrying out its functions, the Anti-Money Laundering Office will pay particular attention to the adequacy of the systems and internal procedures relating to customer due diligence obligations and registration and filing, in addition to the systems for the identification, assessment and reporting of suspicious transactions; to the effective recording of the other situations subject to the communication obligation and to the appropriate filing of the documentation and records required by legislation.

In its assessment of the adequacy of these procedures, the Office will carry out controls, including on a sample basis, to check their effectiveness and functionality and identify any critical areas in agreement with the internal audit function.

More specifically, the Anti-Money Laundering Office:

- will identify the external regulations relating to anti-money laundering and combating terrorism financing;
- will analyse the impact of prevailing law on Bank operations;
- will assess in advance the correct application of all the dispositions regarding anti-money laundering and anti-terrorist measures for all innovative projects (including the operational introduction of new products and services) that the Bank means to embark on, analysing the specific associated risk component and the possible need of taking appropriate mitigating actions;
- will continuously check the adequacy of the management of money laundering and terrorism financing risks process and the suitability of the internal control system and the procedures adopted, and propose any organisational or procedural changes that may be necessary or advisable to ensure adequate control against the associated risks;
- will conduct checks on the functionality of the reporting process and on the adequacy of the assessments made of the customer transactions jointly with the Suspicious Transaction Reporting Manager;
- will collaborate on defining the governance policies of risks of money laundering and terrorism financing and of the various phases making up the process of managing these risks;
- will check the reliability of the information system to meet the obligations of customer due diligence, data filing and reporting suspicious transactions;
- will supervise transmission of the aggregate data relating to the monthly registrations to the Financial Information Unit, meeting any requests by the aforementioned Financial Information Unit, in addition to the objective communications concerning risk of money laundering transactions;
- will perform the self-assessment exercise on the Bank's exposure to the risk of Money Laundering and financing of terrorism on an annual basis, jointly with the other company functions involved, reports the findings to the Board of Directors and implements any consequent corrective operations or those necessary to improve the monitoring systems;
- will lend its support and assistance to the company bodies and to top management;
- will assess the risk of money laundering associated with the offer of new products and services as a precautionary measure;

43 By way of example but not limited to, reference is made to fundraising committees, organisations or entities (whether or not they have legal personality) whose activity is functionally related to that carried out by the political party.

- will provide the HR department with the guidelines to prepare an adequate training plan, aimed at keeping employees and external staff continuously up-to-date;
- will promptly inform the company bodies of significant breaches or shortcomings found when performing its duties;
- will prepare flows of information sent to the company bodies and to top management;
- will monitor the risk classification of the countries based on their national money laundering and terrorism financing prevention systems, and will provide the Foreign Department with the documents necessary to operationally monitor the same risks;
- will provide the anti-money laundering contact person of the Organisation and Systems Area and the anti-money laundering contact persons of the Group companies with the operating instructions and guidelines to carry out their duties properly;
- will guarantee the functional coordination with the Anti-Money Laundering Departments of the Group companies that have not outsourced these activities to the Parent Bank.

Finally, in its capacity as a specialised company supervisor, the Office will interact with the Authorities set up to combat money laundering and terrorism financing.

The Anti-Money Laundering Office Manager will fall within the category of managers of company control departments; he/she will report to the Board of Directors.

In order to guarantee adequate information flows with respect to all the company bodies, the Anti-Money Laundering Office Manager will draw up:

- on a yearly basis, a report on the activities carried out and the critical issues which emerged. This document (i) describes all activities undertaken, the verified failures and the corrective action that needs to be taken; (ii) describes the training programs implemented for personnel; (iii) provides a thorough account of the outcome of the self-assessment exercise and any updating initiatives that have been adopted or planned; (iv) must contain the plan of action for the coming year;
- on a quarterly basis, a Dashboard containing a summary of the results of the activities carried out by the Anti-Money Laundering function and a progress report on the measures adopted in order to overcome the most critical aspects noted.

These documents shall be submitted to the Control and Risk Committee, the Board of Directors, the Board of Statutory Auditors, including in its capacity as Supervisory Board pursuant to Legislative Decree 231/01 to the AISCI and the Managing Director, forwarded to the Heads of the control functions and Bank of Italy officers.

9.7 Group Appointee in charge of suspicious transaction reporting

The Anti-Money Laundering Office Manager will also act in the capacity of *person authorised to report suspicious transactions* on behalf of the Group's companies that have granted him/her appropriate powers; in this context, he/she will have to

- assess, in light of all elements available, suspicious transaction reports that come from the operating units and the Group Companies that have delegated these activities;
- assess, in light of all elements available, the suspicious transactions they have become aware of as part of their activity;
- send those deemed well-founded to the Financial Information Unit, while omitting specification of the names of the subjects involved in the transaction reporting procedure;
- keep a record of the assessments made as part of the procedure, even if the report is not sent to the Financial Information Unit.

In order to carry out his/her functions, the Anti-Money Laundering Office Manager acquires all helpful information from the structure that performs the first level of analysis of the anomalous transactions; will have full access to all the information necessary to perform the activities assigned to the Office and to assess the reports. In addition, he/she will deal with the Financial Information Unit, providing prompt feedback to any requests for further investigation it makes.

Finally, considering the particular relevance that said information could have when opening new accounts or assessing transactions carried out by previously existing customers, the Anti-Money Laundering Office Manager may allow the names of the customers involved in the suspicious transaction reports to be known to the heads of certain company operating structures both through access to appropriate sources of information, and the specific information flows. The recipients of this information are bound to maximum confidentiality in their processing, to not disclosing it to third

parties and to use it only for the purpose of monitoring the risk of money laundering/terrorism financing. In any case, the protection of confidentiality of the identity of the first level parties who make the reports must be guaranteed.

9.8 Figures in other Operating Units / Group Entities

With the intention of supporting the Anti-Money Laundering Office in preventing and combating the money laundering and terrorism financing risks, specific responsibilities are assigned to certain figures in the other Bank operating units, or at subsidiaries that outsourced the anti-money laundering activities to the Parent Bank on the basis of a specific "Service Agreement".

Specifically:

9.8.1 Anti-Money Laundering contact person in the Organisation and Systems Area

- will monitor - with the assistance of the managers of each sector/sub-system giving information to the Central Computer Archive - the correct function, parameterization and update of the information systems underlying the requirements regarding the combating of money laundering and terrorist financing, monitoring the organisational - procedural actions requested/planned for the individual aspects (functional analyses, testing and production releases, SAL, timeframes, developments in course, etc.) and ensuring they are entered within the Organisational Master Plan;
- will interact with the IT outsourcers, monitoring - with the support of the managers from each sector/sub-system giving information to the Central Computer Archive - the procedural releases made that impact on the anti-money laundering aspects (identifying the sub-systems involved, table implementations, logical safety, etc.) and informing the Head of the Anti-Money Laundering Office of any anomalies encountered;
- will support - along with the managers of each sector/sub-system providing information to the Central Computer Archive - the departments in charge of preparing/updating the applicable internal regulations, in particular with respect to the Anti-Money Laundering operating procedures and related applications (for example GIANOS, Central Computer Archive, New Branch, General Data Register, etc.).

9.8.2 Anti-Money Laundering Contact Persons of the Group Companies

Appointed resources at the subsidiaries that provide support for the Anti-Money Laundering Office as described in the relative Service Agreements, operate in close functional coordination with the Anti-Money Laundering Office of the Parent Company within the context of the provisions of the Supervisory Authority (Bank of Italy Provision of 26 March 2019), also with powers of initiative and drive acknowledged by the aforementioned regulations.

Besides the activities detailed above, the Anti-Money Laundering Contact Persons oversee the processes connected to the anti-money laundering regulations acting as support, even for coordination purposes, for the resources relocated by the Parent Company, with particular reference to:

- procedure for the reporting of suspicious operations, for the subsequent forwarding to the Group Manager, subjecting them to analyses;
- the correct execution of the activities related to the customer due diligence by the network;
- assessments regarding relationships with customers whose risk profile has risen higher;
- drafting of the regular reports on activities performed;
- standard oversight activities as defined in the Consolidated Anti-Money Laundering Law.

In the performance of these activities the contact persons functionally respond to the Anti-Money Laundering Contact Person of the Parent Company.

9.9 Internal Audit Committee

The **Internal Audit Committee** continuously checks the level of adequacy of the company organisational set-up and its compliance with the matter in question. It monitors the functioning of the entire internal control system to prevent money laundering and terrorism financing risks.

In accordance with the provisions of the measure - on the basis of its audit plan - it will assess the following through systemic controls, including inspection type controls:

- constant compliance with due diligence obligations, both when opening accounts and as relationships develop over time;

- the actual acquisition and orderly filing of the data and documents provided under the law, based on the provisions of the legislation;
- the actual level of involvement of the employees and external staff, in addition to the managers of the central and external departments in fulfilling their "active collaboration" obligations.

The inspections, including both remote[44] and on-site, will be planned to ensure that all Bank areas will be inspected over an appropriate time period, and the initiatives will be more frequent for the areas with greater exposure to the risks of money laundering and terrorism financing, and with reference to the "high" risk profile accounts.

More specifically, the Anti-Money Laundering Office can delegate - through specific service agreements - the on-site inspections to the Internal Audit Committee in order to avoid duplicating the work, and ensure greater efficiency in the controls, thanks also to the inspection instruments available to the Committee. The result of this activity will be reported on a regular basis.

The Internal Audit Committee also carries out follow-up actions in order to ensure that the corrective actions to the shortcomings and irregularities encountered have been adopted, and ensures that they are suitable to avoid similar situations in the future. The Committee will report any shortcomings found that could have an impact on monitoring the actions taken to combat money laundering and terrorism financing to the company bodies and the Anti-Money Laundering Office Manager.

9.10 Risk Management Department

Updates the "Risk Appetite Framework – RAF" documents and the "Company risk management policy" based on the results posted by the self-assessment exercise, and calls for money laundering risk monitoring indicators that are integrated on the Dashboard that the Management regularly submits to the Board of Directors.

9.11 Compliance Office

With reference to the monitoring of the risk of money laundering and the financing of terrorism, the Compliance Office constantly provides to management with an appropriate management of the risk of non-compliance to which the Bank is exposed, based on the methods detailed in the "Compliance risk management policy".

9.12 Other Business Units

All the Bank's Business Units are responsible - in accordance with and within the limits indicated in the internal procedures - for the due diligence activities, filing, recording the information on the Central Computer Archive and identifying, assessing and reporting suspicious transactions. The Managers of these units will carry out line controls aimed at ensuring compliance by its resources of the internal procedure provisions, including the protocols issued when the 231 Organisational Model was implemented by the Bank, and are responsible for assessing and forwarding to the Group Representative suspicious transaction reports entered into the application also used by the collaborators of the operating unit.

More specifically: (i) the Resource Committee will take part in monitoring the risks of money laundering and terrorism financing through the Human Resources Office, which prepares and checks the training and instruction programs in order to ensure that staff are kept constantly up to date; (ii) the Foreign Department by aligning the IT procedures with the country risk classification prepared by the Anti-Money Laundering Office and through the controls and monitoring defined in its Process Regulation; (iii) the Operation Area supervises certification of the names included on the black lists / lists of PEPs and control over the counterparties of the funds transfer provisions.

44 With reference to these control activities, the Internal Audit Committee will use a remote analysis systems, based on indicators which provide summarised scoring of the risk associated with the Bank Branches.