Policy for preventing and combating money laundering and terrorism financing

March 2018, updated April 2020

Contents

1. Premise

1.1 Objective

This "Policy for preventing and combating money laundering and terrorism financing" (in brief: "AML policy") sets out to ensure that Banca UBAE S.p.A. (hereinafter "Bank") complies with regulatory provisions on preventing and combating money laundering and terrorism financing, applying a risk-based approach, has an organizational structure, operational and control procedures, as well as IT systems suitable to guarantee compliance with the laws and regulations on anti-money laundering[1], taking into account the nature, size and complexity of the activities carried out, as well as the type and range of services provided.
To this end, the AML policy defines the reference principles for the Bank and identifies the main roles and responsibilities of the corporate structures involved in preventing and combating money laundering (AML) and terrorism financing (CFT).

1.2 Validity and field of application

The AML policy comes into force on the day it is approved by the Bank's Board of Directors, after consulting the Board of Statutory Auditors. Any change or updating of the AML policy must be decided by the Bank's Board of Directors after consulting the Board of Statutory Auditors.
All employees and collaborators of the Bank, as part of their work, are required to comply with the contents of this document.

1.3 Regulatory context for preventing and combating money laundering and terrorism financing

For the purposes of preventing and combating money laundering and financing of international terrorism, new regulations have been issued in recent years by the EU and Italian authorities.

Internationally, the main reference legislation is made up of:

- The Recommendations prepared by the International Financial Action Group (FATF) represent the fundamental standards for preventing and combating money laundering and terrorism financing are accompanied by "Interpretative Notes" which form an integral part of the new standards.

At the EU level, the main reference legislation consists of:

- EU Directive no. 2015/849 issued by the European Parliament and Council of 20 May 2015 on preventing use of the financial system for money laundering and terrorism financing, which modifies EU Regulation no. 648/2012 of the European Parliament and Council, repealing Directive 2005/60/EC of the European Parliament and Council and Directive 2006/70/EC issued by the European Commission (known as "IV Directive on anti-money laundering");

- EU regulation 2018/843 issued by issued by the European Parliament and Council of 30 May 2018, which modifies EU Regulation no. 2015/849 on preventing use of the financial system for money laundering and terrorism financing and which modifies Directive 2009/138/EC and 2013/36/EU ("V Directive on anti-money laundering");

- EU delegated regulation no. 2016/1675 issued by the European Commission on 14 July 2016 which supplements EU Directive no. 2015/849 of the European Parliament and Council, identifying high-risk third-party countries with strategic weaknesses;

[1] Since all the obligations contained in the primary national anti-money laundering legislation are envisaged both for the fight against money laundering and for the fight against the financing of terrorism, in this document any reference to the anti-money laundering purpose or to the risk of money laundering must always be understood as including the purpose. to fight terrorist financing. Lastly, the measures referred to in this document are intended to be applied also in contrasting the financing of the programs for the development of weapons of mass destruction.

- Joint guidelines issued on 26 June 2017 by the European Oversight Authorities (EBA, ESMA and EIOPA) regarding simplified and enhanced customer due diligence measures and risk factors;

In Italy, the main reference norm is represented by:

- Legislative decree no. 231 of 21 November 2007, as last amended by legislative decree no. 90 of 25 May 2017, on "Implementing EU Directive 2015/849 on preventing use of the financial system for money laundering and terrorism financing, amending directives 2006/60/EC and 2006/70/EC and implementing EU regulation no. 2015/847 on information data accompanying transfers of funds, repealing EC Regulation no. 1781/2006 (hereinafter: legislative decree 231/2007);

- Legislative decree no. 109 of 22 June 2007 containing measures to prevent, oppose and repress terrorism financing and the activities of countries that threaten international peace and security, as latterly amended by the aforementioned legislative decree no. 90/2017;

- Legislative Decree 4 October 2019, no. 125 relating to amendments and additions to legislative decrees 25 May 2017, no. 90 and no. 92, implementing Directive (EU) 2015/849, as well as implementing Directive (EU) 2018/843 amending Directive (EU) 2015/849 relating to the prevention of using the financial system for money laundering or terrorism and amending directives 2009/138 / EC and 2013/36 / EU

- Provision of Banca d'Italia on 26 March 2019 containing "Provisions regarding organization, procedures and internal controls aimed at preventing the use of intermediaries for money laundering and terrorism financing purposes" (hereinafter: "Organization and AML control provision");

- Banca d'Italia provision of 30 July 2019 containing provisions on customer due diligence to combat money laundering and terrorist financing;

- Banca d'Italia provision of 24 March 2020 containing provisions for the conservation of the making available of documents, data and information for the fight against money laundering and terrorism financing;

- Provision of the FIU, containing "Instructions on objective communications" of 29 March 2019;

2. Definitions and principles

2.1 Definitions

According to legislative decree no. 231/2007, the following actions – if committed intentionally – constitute "**money laundering**":

- the conversion or transfer of assets, knowing that they originate from a criminal activity or from participation in such activity, in order to conceal or disguise the illicit origin of the assets themselves or to help anyone involved in such activities to avoid the legal consequences of their actions;
- concealing or disguising the real nature, origin, location, disposition, movement, ownership of the goods or rights thereon, made knowing that such assets come from a criminal activity or from participation in such activity;
- purchasing, holding or using goods knowing that such assets, at the time of receipt, come from a criminal activity or from participation in such activity;

- participating in one of the acts referred to in the previous points, the association to commit this act, the attempt to perpetrate it, the fact of helping, instigating or advising someone to commit it, or facilitating its execution.

The knowledge, intention or purpose, which must constitute an element of the above actions, can be deduced from objective factual circumstances.

Recycling is considered as such even if the activities that generated the goods to be recycled took place beyond the national borders.

On the other hand, pursuant to article 648-ter.1 of the Criminal Code, "**self-money laundering**" means that the person who has committed or contributed to committing a non-culpable crime, uses, replaces, transfers into economic and financial activities, entrepreneurial or speculative, the money, the goods or other utilities arising from such a crime, so as to effectively hinder the identification of their criminal origin.

Pursuant to legislative decree no. 231/2007, "**financing terrorism**" means any direct activity, by any means whatsoever, to supply, collect, fund, broker, deposit, hold or disburse, in any way, funds and economic resources, directly or indirectly, in whole or in part, usable for the accomplishment of one or more channels with terrorism purposes according to the penal laws, regardless of the actual use of funds and economic resources for the accomplishment of the above channels.

The expression "**high-risk third countries**" refers to countries outside the European Union whose legal systems present strategic deficiencies in their respective national schemes for the prevention of money laundering and terrorism financing, as identified by the European Commission in the exercise of the powers referred to in articles 9 and 64 of the IV AML Directive.

The expression "**third countries**" means countries not belonging to the European Economic Area.

2.2 Principles

2.2.1 Premise

The Bank's governance system for combating money laundering and terrorism financing is based on the value of integrity – pursuing the objectives with honesty, fairness and responsibility, in full and substantial compliance with the rules and the spirit of the applicable legislation – as well as on some guiding principles aimed at defining a systematic and functional framework.

The Bank will work to ensure that:

- the systems and procedures adopted also comply with the provisions and guarantees established by the legislation on personal data protection;
- the measures taken are objectively proportionate to the risk of money laundering or terrorism financing in relation to the type of customer, the continuous relationship, the operation, the product or the transaction;
- the application of the measures envisaged in this regard are also proportionate to the specific nature of the Bank's activity and its scale.

2.2.2 Prohibitions and operating limits

The Bank cannot accept availability of funds which it knows or presumes they arise from actions that could be considered as "money laundering" or "terrorism financing".

Likewise, the Bank cannot entertain relationships with businesses or individuals which it knows or presumes that they finance terrorism or constitute a criminal organisation, belonging to it or supporting it.

Moreover, in compliance with the current internal regulation is forbidden to:

- opening or holding, even indirectly, of corresponding accounts with "banks of convenience"[2]
- opening of any type of account in an anonymous form or with a fictitious holder, nor the use, in any form, of accounts of such type opened in foreign countries.

Lastly, with reference to third-party high-risk countries, the Bank:

- abstains from establishing continuous relationships or executing transactions (and terminates existing relationships) which directly or indirectly involve trust companies, foundations, anonymous companies or subsidiaries, controlled through bearer shares established in high-risk third-party countries.
- these measures also apply to other legal entities, bearing other names, established in the above countries, whose actual holder cannot be identified or their identity verified.
- does not use third-party entities established in these countries, in order to carry out customer due diligence and proper verification;

In consideration of specific operations, the countries of reference and the range of services and products offered, the Bank generally favours the establishment of continuous relationships and occasional transactions with customers connected to its institutional activity.Any requests to open continuous relationships with physical customers and companies not related to the Bank's activities will be assessed on a case-by-case basis upon General Manager authorization and the prior opinion of the anti-money laundering function taking into account the underlying risks and the control actions required.

In this context, also considering the underlying risk profiles, the Bank does not operate with particular categories of customers such as Money Transfer, charitable and non-profit organizations, betting companies. It also does not carry out transactions in virtual currencies or involving anonymous companies (or controlled through bearer shares) or concerning armament materials or gambling[3].

The Bank also established that the opening of relations with:

1) correspondent banks operating in third countries and third countries with high risk;

2) trusts, trust companies operating in third countries;

3) companies operating in sectors with a high risk of money laundering and terrorism financing such as buying gold, public procurement, health, construction, defence, mining, offshore companies

is subject to the authorization of the General Manager, prior the opinion of the Anti-Money Laundering Dept. which assesses the exposure to the risk of money laundering in relations and operations with these entities and the degree of effectiveness of the corporate controls in place to mitigate the risk, suggesting any operating limits.

With specific reference to correspondent relationships[4], the Bank:

• does not accept the opening of "so-called "nested account"[5], of passing accounts, or the use of an account in the name of a respondent by an entity that falls within its group;
• does not accept the opening of relationships with respondents residing in countries with which it does not intend to have any type of direct or indirect connection (from time to time expressly indicated by the Board of Directors) nor to allow payments to be made to other accounts involving subjects belonging to these countries;

[2]The expression "bank of convenience" (or shell bank, shadow bank), pursuant to article 1, paragraph 2, letter(d), of legislative decree 231/2007, means "the bank or body that performs similar functions to a bank but does not have a significant workforce and management structure in the country in which it was established and authorised to exercise activity, nor is it part of a financial group subject to effective supervision on a consolidated basis".

[3] The Bank has adopted a Payment Policy which governs the limits and prohibitions relating to certain areas or matters, reported in the document "Correspondent banks guidelines" approved by the 239th Board of Directors of 23 February 2018.

4 The operativity with correspondent bank is regulated by "Correspondent banks guidelines" approved by the 239th Board of Directors of 23 February 2018.

[5] The expression "nested account" means an account made out to the respondent opened at the correspondent bank that can be used by other responding banks that have a relationship with the respondent but not with the correspondent bank where the account is held. In other words, the correspondent bank indirectly provides services to other banks that are not the respondent.

• do not use correspondent accounts to process certain payment categories explained in the document attached to the correspondent account contract stipulated with the respondent (for example, armaments transactions, money transfers, charities).

The Bank also pays close attention to dual-use items, as well as to new products or services that may be considered likely to be used for the purposes of (i) financing the proliferation programs of weapons of mass destruction and handling of hazardous chemicals, (ii) circumvention of additional specific or general commercial restrictions (export and import ban) or financial restrictions (freezing of goods and resources, prohibitions concerning financial transactions, restrictions on export credits or investments) envisaged towards risky territories and (iii) financing of operations concerning the trade or production of weapons or armament systems.

The Anti-Money Laundering department may propose further operating limitations, to be formalized in the internal regulations, with regard to particular subjects, sectors, products, services and high risk operations, identified on the basis of the communications and information made available from time to time by the Oversight Authorities and by national and international bodies.

2.2.3 Assessment of the risk of money-laundering and financing terrorism

The Bank fulfils annually the analysis of context and operations in terms of ML/TF risks, pursuant to article 15 of legislative decree no. 231/2007, taking into account the risk factors associated with:

- type of customer;
- geographic area of operations;
- distribution channels;
- products and services offered.

On the basis of the identified risks, the Bank adopts safeguard measures and implements the controls and procedures of risk limitation.

The Bank conducts the self-assessment on the basis of a methodology which, consistently with the indications provided by Banca d'Italia, includes the following macro-activities:

1) identification of the inherent risk

2) analysis of vulnerability

3) determination of residual risk

4) remedial action.

The self-assessment is carried out by assessing the exposure to the risk of involvement in money laundering phenomena for each business line considered relevant, taking into account the nature of the Bank, its organization, specific activities and operational complexity.

In the self-assessment document, the Bank gives an account of the reasons that led to the identification of the specific business lines and the weight attributed to each line with respect to overall operations.

In the event of opening new business lines, the Bank conducts the self-assessment for these new lines.

The self-assessment exercise is promptly whenever new significant risks emerge or significant changes occur in existing risks, in operations or in the organizational or corporate structure.

2.3 Customer Due Diligence Management of money laundering and terrorism financing risks

2.3.1 Risk-based approach and customer profiling

In compliance with the risk-based principle contained in the legislation, the Bank modulates the intensity and extent of the due diligence obligations according to the degree of risk associated with the customer.

To this end, the Bank considers the general criteria indicated by the reference legislation for assessing the risks of money laundering and terrorism financing associated with customers and for profiling them.

In particular, it takes into account the following:

1) High-risk factors concerning the customer, the executor and the beneficial owner:

- the type of subject (and/or its legal nature) and its characteristics;

- the country or geographic area of origin (including funds), business relationships, the activity carried out and the countries with which there are significant connections, the economic and financial profile (in terms of income and assets);

- uncooperative or reluctant behaviour in providing information;

- negative reputational indices (e.g. criminal proceedings or for administrative liability, previous reports of suspicious transactions);

- structures that can be classified as asset interposition vehicles such as trusts, trust companies, foundations;

- the inclusion in the lists of persons and entities associated with terrorism financing activities envisaged by EU Regulations or by the ministerial regulations adopted pursuant to legislative decree no. 109/2007;

- type of economic activity (e.g. oil, health, construction, public procurement, defence, arms trade, extractive industry);

- presence of a politically exposed person (PEP) or in any case holding a public office.

2) High-risk factors concerning the complexity of the relationship and the operation:

- type of product or service and their structure (assessed in terms of complexity and transparency), the channels used for their distribution, the possible involvement of multiple parties;

- any commercial triangulations;

- the amount, frequency and volume of transactions;

- the reasonableness of the ongoing relationship or of the transaction[6] in relation to the activity carried out and the overall economic and financial profile of the customer (and of the actual beneficial owner) and the geographical area of destination of the funds;

- any new or innovative service products and those that allow frequent recourse to cash or that allow the execution of transactions of a particularly high amount;

- cash payment transactions from abroad for an amount equal to or greater than 10,000 euro.

[6] With reference to Trade Finance operations, for the purposes of risk assessment, the sectoral risk factors provided for by the EBA connected to the customer, the transaction and the subjects and countries involved in the operations must be considered. CFR Internal procedure n.35 of 9 August 2019.

3) High-risk factors concerning the geographical area:

- customers residing in high-risk geographical areas;
- countries with a high level of corruption or lacking effective anti-money laundering measures;
- countries subject to sanctions or embargoes.

In consideration of the above criteria, a risk profile is assigned to the customer managed also through the support of a specific IT application. Each customer and relationship is assigned one of the following **four levels of risk: irrelevant, low, medium, high**.

The risk profile is assigned or updated when:

- opening an ongoing relationship;
- carrying out an operation that is relevant for anti-money laundering purposes;
- processing monthly performed by the profiling system;
- specific events such as, for example, the acquisition of the PEP qualification, criminal investigations / financial investigations, changes in the corporate structure (e.g. shareholdings of trust companies and/or trusts), change of activity (in risk sectors), news reports relevant to the anti-money laundering purposes, sending reports of suspicious transactions, change of residence to high-risk third countries.

2.3.2 Customer due diligence obligations

The Bank fulfils the customer due diligence obligations according to the relationships and operations that fall within its institutional activity when:

• the customer requests the establishment of an ongoing relationship;
• the customer arranges for the execution of an occasional operation that involves the transmission or movement of means of payment of an amount equal to or greater than 15,000 euro regardless of whether it is carried out with a single transaction or with multiple transactions that appear to be connected for performing a split operation.
• the customer arranges for the execution of an occasional operation that involves a transfer of funds in excess of 1,000 euro;
• whenever there is a suspicion of money laundering or terrorism financing regardless of any applicable derogation, exemption or threshold;
• when there are doubts about the completeness, reliability or truthfulness of the information or documentation acquired for the purpose of customer due diligence.

In order to ensure the correct fulfilment of customer due diligence obligations, the competent structures carry out:

• identification of the customer and, where present, the executor and the beneficial owner, through the acquisition of identification data and information, as well as the collection of copies of identification documents; the reconstruction, according to a risk-based approach, of the ownership and control structure of customers other than a natural person, in order to find, with reasonable certainty, the identity of the effective owner declared by the executor at the time of identification;
• verification of the data relating to the customer and, where present, the executor and the beneficial owner, by checking the veracity of the identification data and the information acquired at the time of identification, evaluating the extension according to a risk-based approach and the depth of the checks to be carried out;

• the acquisition and evaluation of information on the purpose and expected nature of the ongoing relationship, on the relationships between the customer and the executor and between

the customer and the beneficial owner, as well as on the work and economic activity carried out and, in general, to the business relationships of the customer and the beneficial owner;
• the conservation of the documentation acquired during adequate verification;
• the exercise of constant control during the ongoing relationship through:

1. the identification, by examining the customer's overall operations and the possible acquisition of further significant information for the purpose of assessing the risk of money laundering of elements inconsistent with the customer's economic and financial profile;
2. the periodic updating of identification data and information relating to customers according to the frequency determined by the risk profile, as well as on the occasion of the acquisition of particular qualifications (e.g. PEP).

The Bank has established the following periodicity for the revision of the assigned risk profile: half-yearly for high risks, annual for medium risks, three-year for low risks and five-year for low risks.

The review also takes place when events deemed significant for the purpose of money laundering or terrorism financing occur.

1-Enhanced due diligence obligations

The Bank will apply the enhanced due diligence procedure in the presence of a high risk of money laundering and terrorism financing in the cases provided for by the regulatory provisions or consideration of the independent assessment of the customer profile on the basis of the risk factors.

In particular, the standard always considers high risk:

a) customers residing in high-risk third countries identified by the European Commission;

b) cross-border correspondent relationships with a credit institution or financial institution of a third country;

c) ongoing relationships or transactions with customers and their beneficial owners who are politically exposed persons;

d) customers who carry out operations characterized by unusually high amounts or in respect of which there are doubts about the purpose for which they are, in concrete terms, destined.

In addition, the Bank will carry out the adequate reinforced verification for the continuous relationships characterized by the aforementioned criteria relating to the customer, the executor and the beneficial owner, the products, services and distribution channels and the geographical area of reference.

In order to ensure strict monitoring of the above relationships, the Bank has established that, if at the end of the enhanced due diligence procedure the presence of risk factors - as indicated above - which have engaged this procedure is confirmed, the position is always attributed a high risk.

Enhanced due diligence measures imply:

a) the acquisition of more information relating to:

- customer and beneficial owner (verification of ownership and control structure; evaluation of reputation information relating to proceedings or sanctions, activities carried out in the past and business or family ties found in the media or from reliable open sources);

- ongoing relationship with specific regard to nature and purpose (analysis of the number, extent and frequency of operations to highlight possible inconsistencies; reasons for which the customer requests a specific product when his needs could be met in another way or another country);

- destination of funds (both the country and the purpose of use);

- the nature of the activity carried out.

b) better quality of information:

- verification of the origin of the assets and funds used in the ongoing relationship (examination of financial statements, tax returns; in case of high use of cash, verification of consistency with the activity carried out and turnover; in the case of operations with large banknotes, insights into the reasons behind this operation);

c) higher frequency of updates:

- checks on the ongoing relationship to detect any changes in the customer's risk profile;

- more frequent checks on operations to detect any elements of suspicion of money laundering (e.g. destination of funds and reasons for a given operation).

d) authorization of the General Manager to start or continue the ongoing relationship.

In addition, in order to ensure constant monitoring of ML/TF risk, in the event of activation of the enhanced due diligence procedure, the Bank provides for an authorization procedure which, in addition to the involvement of the hierarchical managers of the Business areas and the General Management, requires the intervention of the Anti-Money Laundering Unit in the presence of a particularly high risk profile.

The Bank also pays particular attention to frequent cash transactions through careful monitoring and the determination of amount thresholds for payment and withdrawal transactions over a limited period of time, after which the opportunity to maintain the relationship must be assessed, raising the customer's risk profile[7].

With particular reference to ongoing relationships or transactions with customers and beneficial owners who are **politically exposed persons**, except as indicated above, the Bank has established that:

- PEPs are always attributed a high risk, as well as subjects related to them, even if not expressly considered by the reference legislation (e.g. delegates / delegates and co-holders of continuous relationships);
- in order to check the status of PEP (both during the opening phase and during the monitoring phase of a relationship), in addition to the information provided by the customer, further sources such as official authority websites or commercial databases can be used by the Bank or other information already collected in other locations (e.g. granting a credit line). The extension of the checks is commensurate with the degree of risk associated with the product or operation requested;
- The consent and maintenance of a relationship with a PEP is expressly approved by the General Manager, who assesses the exposure to the risk of money laundering of the PEP and the effectiveness of the risk mitigation measures adopted by the Bank;

- in the event of a particularly high risk of money laundering, it is appropriate to continue to apply the adequate reinforced verification, even if the PEP has ceased to hold public office for over a year;
- enhanced due diligence measures involve the acquisition of the information necessary to establish the origin of the PEP assets and the funds used in the relationship or in the transaction. For this purpose, the customer's attestation must be verified on the basis of reliable documents from independent sources, provided by the customer himself or publicly available;
- the checks are intended to exclude that the funds used are the result of crimes of a corrupt nature or other criminal cases; these elements together with the customer's reluctance to provide information can be the subject of a suspicious transaction report;
- at least annually the AML unit, in the context of reporting to the Board of Directors, assesses the Bank's exposure to the ML/TF risks associated with PEPs.

[7] The 241st Board of Directors of 27 March 2018 approved a "Cash Policy".

2-Simplified due diligence obligations

In cases of low risk of money laundering, simplified adequate verification measures can be applied if there are:

a) low-risk factors relating to the customer, executor and beneficial owner:

- companies admitted to listing on a regulated market;
- public administrations or bodies that perform public functions according to European Union law;
- customers or beneficial owners resident in low-risk geographical areas;
- EU banking and financial intermediaries or residents of a third country with an effective system to combat money laundering and terrorism financing (provided that the intermediary has not been subject to supervisory sanctions for non-compliance with anti-money laundering obligations).

b) low-risk factors relating to products, services, operations or distribution channels:

- products or services that suitably defined and limited to certain types of customers, aimed at promoting financial inclusion;
- products whose risks of money laundering or terrorism financing are mitigated by certain conditions such as the spending limit or the transparency of ownership and which therefore do not lend themselves to being exposed for illicit purposes (e.g. products with limited functionality with a predetermined threshold of operations or which do not allow anonymity or concealment of the identity of the customer or beneficial owner).

c) low geographical risk factors:

- EU countries;
- third countries with an effective system to combat money laundering and terrorism financing at a level similar to that provided for by the European Anti-Money Laundering Directive;
- third countries characterized by a low level of corruption;
- third countries that on the basis of authoritative sources (FATF; Moneyval) are equipped with an effective system for the prevention of money laundering and terrorism financing.

Simplified adequate verification measures lead to a reduction in the extent and frequency of checks with reference to:

- the timing for the identification of the customer and the effective owner: the identification data can be collected before the opening of the relationship, postponing the acquisition of a copy of the document up to a maximum of thirty days;
- the reduction of the information to be collected: verification of the data referred to the beneficial owner by acquiring a declaration signed by the customer;
- the reduction of the updating of the data collected for adequate verification in certain circumstances (e.g. in the event of opening a new relationship);
- the reduction of the frequency and depth of relationship monitoring: e.g. constant control only for transactions for amounts exceeding a certain threshold.

It is understood that the application of the adequate simplified verification depends on the overall assessment of the customer and their operations; the continuation of the prerequisites for the simplified measures must however always be verified during the relationship. Therefore, should the conditions described above fail or when there is a suspicion of money laundering, the adequate simplified verification does not apply.

3-Additional due diligence measures - Sectoral risk factors

For the purpose of applying the simplified or enhanced due diligence measures, the Bank also takes into account the sectoral risk factors[8] indicated by the reference legislation in relation to the specific activity carried out ("Trade Finance Operations" and "Correspondent Banking Operations").

The assessment of the aforementioned factors must be carried out taking into account the measures of adequate ordinary and enhanced verification adopted towards the customers (banking and corporate) and the counterparties involved in the transaction even if they are not "direct" customers of the Bank (among the checks on the counterparties it is required, for example, the adoption of measures aimed at understanding the ownership or background of the parties involved and the collection of more information on the financial situation of the parties involved).
This process is also relevant from the point of view of active collaboration in that, in strengthening the knowledge of the customer and the underlying transaction, it facilitates the process of identifying suspicious money laundering and/or terrorism financing operations.

The internal procedures illustrate in detail the low and high-risk factors (briefly described below), assessment objects, the activities of "adequate verification of the operation" and of the counterparties involved and the information flows between the structures involved in the operational process:

- **Risk factors related to the transaction**, such as, for example, the lack of consistency of the type and quantity of the goods with respect to what the Bank knows about the customer's business, presence of significant discrepancies in the credit documentation, structured transaction with different subjects involved;
- **Risk factors related to the subjects involved in the transaction** (e.g. presence of indications that the buyer and the seller are complicit);
- **Geographical or country-related risk factors** (e.g. country related to the operation in which currency exchange controls are in force. This, in fact, could increase the risk that the purpose of the operation is the export of currency in violation of local legislation).

2.3.3 Cross-border correspondent relationships with correspondent banking or financial intermediaries from a third country

"Correspondent" means the accounts kept by banks for the settlement of interbank services and other relationships, however denominated, held between credit institutions and financial institutions, used for the settlement of transactions on behalf of the customers of the corresponding institutions.
Transition accounts are cross-border correspondent banking relationships between financial intermediaries used to carry out transactions in their own name and on behalf of customers.
Following the risk-based approach, the enhanced due diligence measures applied towards the correspondent intermediary based in a third country with which a cross-border correspondent current account is established are modulated, paying particular attention, in the risk assessment, to the country where the institution is located.
Before initiating an ongoing relationship with a correspondent body from a third country, by which we mean non-EU countries, the Bank must:

- ensure that the correspondent entity (direct correspondent) is not a convenience bank or an intermediary that allows access to correspondent bank current accounts;
- formalize with the correspondent a written agreement setting out the anti-money laundering terms, obligations, activities and responsibilities that the parties mutually undertake to respect;

[8] Risk factors contained in Title II (Sectoral Guidelines) of the joint Guidelines of the European Supervisory Authorities of 4 January 2018 - See documents "Guidelines on correspondent banking" and "Trade Finance operations".

- acquire further information on the correspondent, also through publicly available information, in order to identify the ownership structures, the nature of the activities carried out and the services offered and to evaluate their reputation and the quality of the supervision to which they are subject;
- evaluate the institution's internal anti-money laundering system by acquiring the internal documentation and, in the event of a high risk, by carrying out further checks;
- acquire the authorization of the General Manager for the opening of any correspondent account;
- activate a constant control of the rapport, grading the frequency and intensity

---

The internal procedures illustrate in detail the methods of enhanced due diligence taking into account the assessment of the riskiness of the high-risk factors referred to in the reference legislation[9].
In particular, risk factors related to:

- products, services and transactions carried out by the respondent bank (e.g. wire transfers, trade finance transactions as indicated in the correspondent contract entered into with the Bank);
- respondent bank's customers (in particular, the respondent bank's anti-money laundering and terrorism financing control policies, the reputation of the respondent bank and its beneficial owner, the sectors of economic activity of the respondent bank's customers);
- geographical area of the respondent bank (for example the respondent bank is based in a country with a higher risk of money laundering, characterized by significant levels of corruption, without effective supervisory action, the respondent performs a significant part of the activities in a country associated with a higher risk of money laundering).

Dispositions concerning remote operations

The Bank, both in opening and monitoring of a relationship, pays particular attention to remote operations, in consideration of the absence of direct contact with the customer or the executor, and alternatively carries out feedback further as indicated below:

a) acquisition of a copy of a valid identity document by fax, post, in electronic format or with similar methods;
b) further checks aimed at avoiding the risk of identity theft or unreliability of the data collected as part of the due diligence process. These additional checks could consist of one or more of the following activities / methods:
   - preparation and filing of a report by the manager of the commercial relationship relating to the on-site visit to the potential client company illustrating the identity of the client and the beneficial owner and the other information collected on the client's ownership and control structure (accompanied by appropriate documentation).
   - sending by the Bank to a physical home with a return receipt of a specific communication requesting confirmation of the data previously sent by the Bank to the customer.
   These documents must be returned countersigned by the customer;
   - verification of residence, domicile, activity carried out, through a special report made by Bank collaborators (duly trained for the purpose) who, after meeting on site with the customer, can certify the authenticity of the identification data communicated by the customer to the Bank.
   - acquisition of a certificate from a lawyer authorized to operate in the client's country of origin where the same, after meeting on site with the client, can attest to the authenticity of the identification data communicated by the client to the Bank;
   - activation of the relationship following the receipt of a transfer from a banking intermediary based in Italy or in a community country where the Customer will have to report the appropriate code communicated to him by the Bank in the description of the reason for the payment.

[9] Risk factors in correspondent banking contained in the joint Guidelines of the European Supervisory Authorities of 4 January 2018 – see note 20

2.3.4 Strengthened controls in the context of international financial sanctions, the fight against the financing of terrorism, and international embargoes.[10]

The Bank is strongly engaged in the fight against the financing of national and international terrorism and adopts appropriate internal procedures and systems to prevent and avoid the establishment (i.e. the continuation) of relationships and the execution of operations with persons suspected of being responsible for terrorism.

To this end, the Bank adopts enhanced control procedures aimed at:

- verifying, through automated procedures, the correspondence between the customer identification data and those contained in the lists (so-called black lists) of the sanctioned subjects, designated by the UN Security Council, by the European Union, by the decrees of the Ministry of Economics and Finance, as well as that of the United States Office of Foreign Asset Control (OFAC); the results of these checks are verified by the personnel in charge in order to ensure the correct functioning of the procedures and to exclude any cases of homonymy (so-called false positives);
- applying asset freezing measures both in the relationship opening phase and in the monitoring phase, towards the subjects for which the identity of the designated subject has been ascertained;
- refusing to carry out operations involving for any reason subjects included in the black lists (e.g. executors, payers, beneficiaries) and confirmed as such;
- requesting additional information in the case of transactions or relationships that present a high risk of being involved in restricted activities;
- communicating to the UIF (Financial Information Unit) the measures applied pursuant to Legislative Decree 109/2007 and subsequent amendments, indicating the parties involved, the amount and nature of the funds or economic resources, within thirty days from the date of entry into force of the EU regulations, of the decisions of the international bodies and of the European Union and of the decrees of the Minister of Economy and Finance, or, if later, from the date of holding of the funds and economic resources.

Regarding embargoes, so as not to incur violation of the legislation in the context of its institutional activities, the Bank adopts measures that ensure:

- registry and transaction checks;
- checks to be carried out for operations coming from or directed to the countries, people and entities to which restrictions are established.
- The Bank applies, where necessary, the financial restrictions established by the national or international reference bodies (e.g. freezing assets and resources, prohibitions of certain financial transactions, prohibitions of documentary operations related to the export of dual-use and/or dangerous goods).

For this purpose, in the context of export transactions, the Bank requests a letter from the credit card exporters stating that the goods are not subject to authorization by the authority, to special restrictive regimes, constraints or prohibitions imposed by national and international regulations (excluding food, medicines in general or other categories valued by the Bank as not subject to risk such as oil and its derivatives).

[10]It should be noted that the Bank has already adopted specific arms and operating policies with embargoed countries (Resolution no. 221 of 16/09/2016 on the ban on operations related to the supply of weapons; resolution of the 196th BoD on 7 February 2014 on USD transactions with countries embargoed by the OFAC; BoD resolution no. 223 dated 16/12/2016 on operations with Iran; BoD resolutions by 234th BD on 27 October 2017, 235th BD on 28 November 2017 and 236th on 21 December 2017 regarding operations with Sudan).

2.3.5 Obligations of conservation

The Bank keeps the documents, data and information useful to prevent, identify or ascertain any money laundering or terrorism financing activities and to allow the analysis to be carried out, within the respective attributions, by the FIU and by the competent Authorities.

The Bank adopts systems for storing documents, data and information suitable for guaranteeing compliance with the rules laid down for the protection and processing of personal data.

The Bank has maintained the Central Online Database (AUI) as a suitable tool for data retention.

2.3.6 Reporting suspicious operations

In order to ensure the control of the operations carried out by customers, the Bank has a specific reporting process which is based on the following activities in compliance with the confidentiality of the reporting party:

- prior to control of the operations carried out by customers, on the basis of the current implementation provisions issued by the Oversight Authorities, in order to identify and block the transactions on which there are suspicions of money laundering and/or terrorism financing;

- after monitoring, on a monthly basis, of transactions in order to identify anomalous operations, through the use of a specific IT application.

In order to ensure compliance with the obligation to report suspicious transactions, the Bank uses a special IT application to identify potential anomalous transactions, as well as an internal reporting procedure that enables traceability of all stages of the process (from the start of the first-level report up to the evaluation and consequent determination by the SOS Manager).

The manager of the dependency, of the office or other operating point or organizational unit or structure of the Bank has the obligation to communicate without delay and where possible before carrying out the operation, the operations deemed suspicious to the SOS Manager when he knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing operations are in progress or being attempted or have been attempted or that the funds, regardless of their size, come from criminal activities.

The suspicion is inferred from the characteristics, the entity, the nature of the operations, their connection or splitting or any other known circumstance, due to the functions performed, based on the elements acquired.

The SOS Manager examines the reports received and, if he deems them founded in the light of all the elements available to him and the evidence inferable from the data and information stored, transmits them to the FIU, without the name of the reporting party.

The Bank takes all appropriate measures to ensure the confidentiality of the reporting person's identity. The SOS Manager is responsible for the safekeeping of the acts and documents which indicate the identity of the reporting person.

It is forbidden for the subjects required to report and to anyone who is in any case aware of it to communicate to the customer concerned or to third parties the occurrence of the report, the sending of further information required by the FIU or the existence or the probability of investigations or insights on the matter money laundering or terrorism financing.

2.3.7 Whistleblowing

With regard to the adoption of suitable procedures for reporting within the Bank (whistle-blowing) by employees and collaborators, of actual or potential violations of the provisions to prevent and

combat money laundering and terrorism financing, the Bank has implemented an internal management process of reports approved by the 214th Board of Directors on 19 February 2016.

2.3.8 Training

Banca UBAE pays particular attention to staff training and instruction, having regard, among other things, to the specific preparation that is required for employees and collaborators who are in more direct contact with customers, as well as the staff belonging to the AML Function, for which specific training sessions are established.

The qualification activity of the Bank's staff in the AML/CFT area is of continuity and systematic nature within the framework of organic programmes, of which information is provided annually, both in terms of programming and in terms of implementation, to the Board of Directors and the Board of Statutory Auditors.

As part of the AML/CFT training, the Anti-Money Laundering Unit and the HR Sector interact actively in order to prepare an annual AML/CFT training programme andshare the method and tools deemed most suitable for delivering the training sessions.

The Bank's anti-money laundering unit also carries out consultancy and specialist assistance on the methods of fulfilling the anti-money laundering and anti-terrorism obligations both towards the operating structures involved and towards the corporate bodies.

3. Roles and responsibilities

3.1 Board of Directors[11]

The Board of Directors, as an organ with strategic oversight function, is responsible for:

- the approval and periodic review of the strategic guidelines and governance policies of the risks associated with money laundering and terrorism financing; in compliance with the risk-based approach, the policies are appropriate to the extent and type of risks to which the Bank is concretely exposed in carrying out its business, as represented in the self-assessment document;

- the approval of a policy that illustrates and motivates the decisions that the Bank takes on the various relevant profiles regarding organizational structures, procedures and internal controls, adequate verification and conservation of data, in accordance with the principle of proportionality and effective exposure to money laundering risk (known as anti-money laundering policy);

- the definition and approval of the guidelines of an organic and coordinated internal control system, functional to the prompt detection and management of the risk of money laundering and ensures its effectiveness over time;

- the approval of the institution of the anti-money laundering sector, identifying the related tasks and responsibilities, as well as the methods of coordination and collaboration with the other corporate control functions;

- the approval of the principles for managing relations with customers classified as "high risk";

- ensure that anti-money laundering tasks and responsibilities are clearly and appropriately allocated, ensuring that operational and control functions are distinct and provided with adequate staffing in terms of quality and quantity;

[11] Second part, Section II, Provision for AML Organization and Controls.

- ensure that an adequate, complete and timely information flow system is prepared for the Bank's corporate and control bodies;

- appoint and revoke the AML Manager and the SOS manager, after consulting the Board of Statutory Auditors;

- ensures the protection of confidentiality within the reporting procedure for suspicious transactions;

- annually, examines the reports relating to the activity carried out by the AML Manager and the controls performed by the competent units, as well as the document on the results of the self-assessment of the risks of money laundering;

- ensure that the deficiencies and anomalies found as a result of the various level checks are brought to its knowledge promptly and promote the adoption of appropriate corrective measures, the effectiveness of which is verified;

- assess the risks resulting from operations with third countries associated with higher money laundering risks, identifying the safeguards to mitigate them, whose effectiveness it monitors.

3.2 General Manager[12]

The General Manager plays a fundamental role in the functioning of the organizational structure with which the Bank is equipped in order to prevent and counter the risk of money laundering and terrorism financing.

The General Manager supervises the implementation of the strategic guidelines and governance policies for the risk of money laundering defined by the Board of Directors and is responsible for taking all the necessary actions to ensure the effectiveness of the organization and of the anti-money laundering control system, in order to ensure compliance with the relevant obligations. In preparing operational procedures, he takes into account the indications and guidelines issued by the competent authorities and international bodies.

In this context, the General Manager defines and supervises the implementation of an internal control system for the prompt detection and management of the risk of money laundering and ensures its effectiveness over time, in line with the evidence drawn from the self-assessment exercise of the risks and ensures that the operating procedures and information systems enable the correct fulfilment of the obligations of customer due diligence and of the conservation of documents and information.

The General Manager is also entrusted with the following tasks:

- defining the anti-money laundering policy submitted to the Board of Directors for approval;

- defining and safeguarding the implementation of the information procedures aimed at ensuring knowledge of the risk factors for all the corporate structures involved and the bodies in charge of control functions;

- approving training programmes and sessions for employees and collaborators on the obligations deriving from the anti-money laundering regulations. The training activity also for the AML Unit must be of a continuity and systematic nature and take into account the evolution of the regulations and internal procedures;

- establishing the appropriate tools to allow the constant verification of the activity carried out by employees and collaborators in order to detect any anomalies that emerge, in

[12] Second part, Section III, Provision for AML Organization and Controls.

particular, in the behaviours, in the quality of the communications addressed to the representatives and to the corporate structures, as well as in the rapports that the employees or collaborators have with customers;

- defining the procedures for managing relations with customers classified as "high risk", in line with the general principles established by the Board of Directors;

- In cases of remote operations (e.g. carried out through digital channels) the adoption of specific IT procedures for compliance with anti-money laundering regulations, with particular reference to the automatic identification of anomalous operations.

With regard to customer due diligence, the General Manager is responsible for approving the opening or maintenance of relationships:

- with customers residing in high-risk third countries;
- with customers and their beneficial owners who are politically exposed persons;
- cross-border correspondence with a credit institution or financial institution of a third country.
- customers who, in consideration of the high risk profile, undergo adequately strengthened due diligence activities

With regard to reporting suspicious transactions, the General Manager is responsible for ensuring that:

- a procedure is defined that is appropriate for the specificity of the activity, the size and complexity of the recipient, according to the principle of the risk-based approach. The procedure is able to guarantee certainty, homogeneity in behaviour and generalized application to the entire structure, the full use of the relevant information and the reconstruction of the evaluation process;the General Manager also adopts measures aimed at ensuring maximum confidentiality on the identity of the persons who participated in the suspicious transaction reporting procedure;
- he also ensures that instruments, including IT tools, are available for detecting anomalous transactions.

Finally, the General Manager is responsible for defining the initiatives and procedures to ensure the timely fulfilment of the communication obligations to the authorities provided for by the anti-money laundering legislation.

3.3 Board of Statutory Auditors[13]

The Board of Statutory Auditors is entrusted with the task of supervising compliance with the legislation and the completeness, functionality and adequacy of anti-money laundering controls. In exercising its powers, the Board of Statutory Auditors makes use of the internal structures for carrying out the necessary checks and verifications and uses information flows from other corporate bodies, the AML Manager and other internal control functions.

The tasks assigned to the Board of Statutory Auditors fall within:

- the assessment, to be carried out with particular attention, of the suitability of the procedures in place for the proper verification of customers, for the storage of information and for the reporting of suspicious transactions;
- stimulate the in-depth action of the reasons for deficiencies, anomalies and irregularities found and promote the adoption of appropriate corrective measures.

[13] Second part, Section IV, Provision for AML Organization and Controls.

The Board of Statutory Auditors is consulted about the appointment of the AML Manager and the SOS Delegate, as well as the definition of the elements of the overall architecture of the money laundering risk management and control systems.

Finally, the Board of Statutory Auditors is called to:

- communicate, without delay, to the SOS Delegate the potentially suspicious transactions of which it becomes aware in the exercise of its functions[14];
- inform the Oversight Authorities without delay of all the facts which they become aware of in the exercise of their functions – facts which may lead to serious or repeated or systematic or multiple violations of the provisions pursuant to Title II of Legislative Decree 231/2007 and related implementing provisions, of which it becomes aware in the exercise of its functions[15].

3.4 Person in Charge of Reporting Suspicious Operations (Corporate Delegate)[16]

The responsibility for conducting the assessment and the possible transmission of reports on suspicious transactions to be forwarded to the UFI, pursuant to article 36 of legislative decree no. 231/2007, is attributed to the person entitled "Corporate Delegate" who, on the date of this document, coincides with Head of AML department.

The Corporate Delegate is in possession of adequate requisites of independence, authority and professionalism, carries out its activity with independent judgment and in compliance with the confidentiality obligations provided for by Legislative Decree 231/2007, also with regards to representatives and other corporate functions.

The Corporate Delegate has no direct responsibilities in operational areas and is not hierarchically dependent on people of such areas.

The Corporate Delegate has free access to information flows to the corporate bodies and the various departments involved in managing and combating money laundering and terrorism financing.

The following tasks are assigned to the Corporate Delegate:

- Assessing, in the light of all available elements, the operations submitted for attention by responsible of dependence or other operative point, of the organisational units, or of the structure responsible to customer relationship (known " first level"), or of which he has otherwise become aware in the context of his business;

- transmitting to the FIU the reports deemed to be founded, omitting the indication of the names of the subjects involved in the procedure for reporting the transaction;

- keeping evidence of the assessment carried out in the field of the procedure, also in the case of no report to the FIU;

- communicating, with the appropriate organizational methods to ensure the respect of the confidentiality obligations provided by Legislative Decree 231/2007, the outcome of its assessment to the subject that gave rise to the report;

- carrying out checks, including by sampling, on the adequacy of the assessments made by the first level on customer operations;

- applying, rigorously and effectively, instructions, schemes and indicators issued by the FIU;

[14] Article 46, c.1, letter b), legislative decree no. 231/2007.
[15] Article 46, c.1, letter b), legislative decree no. 231/2007.
[16] Chapter II, Section II, Provision on AML Department.

- performing an interlocutory role with the FIU and promptly correspond to any requests for further information from the same;
- keeping records and documents showing the details of the person reporting, in order to ensure their confidentiality

The Corporate Delegate can acquire any useful information from the structure that carries out the first level of analysis of anomalous operations; it has free access to information flows directed to significant corporate bodies and structures for the prevention and combating of money laundering; also uses any elements that can be inferred from freely accessible information sources in the assessments.

Without prejudice to the protection of the confidentiality of the identity of the person taking part in the procedure for reporting transactions, the corporate Delegate provides -also through the use of suitable information bases - information on the names of customers subject to reporting suspicious transactions to the responsible of the structures competent for the purpose of assigning or updating the risk profile of the customers themselves.

3.5 Anti-Money Laundering Department [17]

The AML department, which the bank is equipped of , has complex functions, to be exercised transversally on all the operations carried out by the Bank, which can be qualified in terms of both verifying the functionality of procedures, structures and systems, and of support and advice on choices management.

In addition to the independence of the Anti-Money Laundering Function, the Bank continuously ensures that the same is endowed with resources qualitatively and quantitatively adequate for the tasks to be carried out and has economic resources, which may also be activated independently.

3.5.1 Organizational framework

In consideration of its size and operational reality, the Bank has established the AML Department as an autonomous organisational element independent of the operating structures and contacts with customers. Its allocation within the Compliance & Anti-Money Laundering Department takes into account of the distinct separation of activity with personnel dedicated to risk of money laundering.

The AML Department responds functionally to the Bank's Board of Directors, also through the Audit & Control Committee.
Its placement in the Bank's organisation chart requires hierarchical dependence on the General Manager.

3.5.2 Mandate and reference perimeter

The principal mandate of the AML Department is to verify constantly that corporate procedures are consistent with the objective of preventing and dealing with violations of official rules and regulations (regulatory laws and norms) and self-regulation regarding money laundering and terrorism financing. The AML Department forms part of the Bank's internal control system, as part of the risk management control functions (2nd level controls) with the aim of preventing, combating and otherwise reducing the ML/TF risks inherent in the Bank’s operations.

To this end, the AML Department has access to all the Bank’s activities, including outsourced activities, as well as any information relevant to performing the tasks assigned to it.

[17] Part Three, Section I, Provision Organization and Controls AML

The AML Department collaborates with the judicial and police authorities, with the Bank of Italy's Financial Information Unit (FIU), and with all the oversight authorities for matters concerning AML/CFT.

3.5.3 Responsibilities

In order to implement the mandate assigned to it, the Anti-Money Laundering department operates with professional independence and autonomy in compliance with current legislation and the overall direction of the Bank's internal control system, and provides for:

- Identifying the rules applicable to the Bank and assessing their impact on corporate processes and procedures;
- collaborating in the set-up of the internal control system and procedures aimed at preventing and combating money laundering and terrorism financing risks (ML/TF risks);
- on going checking of the adequacy of the money laundering risk management process and the suitability of the internal control system and procedures and propose organizational and procedural changes aimed at ensuring adequate control of money laundering risks ;
- providing advice and assistance to corporate bodies, top management and the Bank's offices.
- In the case of innovative projects including new products or services which the Bank intends to undertake, the Department will carry out ex ante and in advance the proficiency evaluations;
- Collaborating to the definition of government policies of the risk of money laundering and of the different stages in which consists the process of management of such risk;
- coordinating the annual self-assessment of money laundering risks to which the Bank is exposed;
- promptly notifying to the corporate bodies of violation or relevant deficiency found during the exercise of its responsibilities
- preparing direct information flows to corporate bodies and top management;
- participating in the process of evaluation of the risk profile of the clients
- dealing with preparing an adequate training plan aimed at achieving an update on an ongoing basis of the employees and collaborators;
- carrying out enhanced customer due diligence activities in cases where, due to objective, environmental and / or subjective circumstances, the money laundering risk (ML risk) appears particularly high;
- participating in the enhanced customers due diligence activities and eventual beneficial owners identified as politically exposed persons PEP's
- checking the reliability of the informative process for the compliance with the obligations regarding due diligence, data storage and report suspicious operations;
- analysing, for the purpose of assessing the ML/TF risk profile, the requests for bank verifications and the related replies sent to the Anti-Money Laundering Department by the Bank departments involved

- preparing for the General Manager, who submits to the approbation of Board of directors, a document that defines responsibilities, tasks and operating methods in ML/TF risk management; the document is constantly updated and must be available and easily accessible to all employees and collaborators;

- collaborating in updating his document (known as "AML policy");

- submitting annually to the Board of Directors, through the Audit & Risk Committee, to the Board of Statutory Auditors, a report on the initiatives undertaken, on the malfunctions detected and the relative corrective actions to be undertaken, as well as the training activities for the personnel; the report also contains the plan of activities and the self-assessment ;

- collaborating with the authorities cited in title I, chapter II of legislative decree 231/2007. With regard to the request from legal authorities and investigative authorities, the Department manages the accesses and the request, prepares feedback and storages the documentation

3.5.4 Head of Anti-Money Laundering Department

The Head of the Anti-Money Laundering Department (hereinafter AML Manager) must possess adequate qualifications of independence, authority and professionalism. The job entails complex responsibilities to be exercised across the Bank's entire range of operations, in terms of checking the functionality of procedures, structures and systems, and providing support and advice on management decisions, subject to the fact that the AML Department cannot have direct responsibility for operating areas nor be hierarchically dependent on persons responsible for these areas.

In consideration of the importance of the tasks assigned and in order to ensure the stability and independence of the AML Manager, the Bank has decided that the appointment and revocation of the manager is of strict and non-delegable relevance to the Board of Directors, after consulting the Board of Statutory Auditors which reports to the Board of Directors, also through the Audit & Risk Committee.

At the present time, the AML Manager coincides with the Head of the Compliance & Anti-Money Laundering Department and also in charge of reporting suspicious operations (known "Corporate delegate").

With reference to the duties assigned to the Anti-Money Laundering Department outlined in the previous section, the activities directly related to the AML Manager are listed below:

- reporting periodically on activities carried out, to the Board of Directors, through the Audit & Risk Committee, and to the Board of Statutory Auditors;

- reporting any anomalies or irregularities concerning the organisational model and the Bank's code of conduct, detected during the verification process, to the Board of Statutory Auditors, also in its function as Oversight Body pursuant to decree no. 231/2001;

- informing the General Manager promptly and, where appropriate, the Chairman of the Board of Statutory Auditors and the Chairman of the Internal Control Committee, of any behavioural anomalies and/or irregularities found during the course of the checking.

On the subject of reporting suspicious operations, the AML manager, as Corporate delegate, is required to:

- evaluate the reports of suspicious transactions received;

- once the suspicious transaction has been reported, the AML Manager speaks with the FIU and possibly with the judicial police bodies responsible for investigating, promptly complying with requests for further information;

- ensures the conservation, for ten years, of the documentation and evidence relating to the internal processes for detecting anomaly indices, and assessing the existence or not of the conditions for starting the internal process of reporting a suspicious transaction;

- coordinates the automatic detection process of potentially anomalous operations;

- deals with filing the documentation relating to the SOS reported, in compliance with the measures identified to ensure confidentiality.

Without prejudice to protecting the confidentiality of the identity of the person taking part in the procedure for reporting transactions, the corporate delegate can disclose the names of the customers involved in the report of suspicious transactions and allow them to be consulted – also using appropriate databases – by the managers of the various corporate bodies concerned, given the particular significance that this information can have during the opening of new contractual relationships or the assessment of operations by existing customers.

3.5.5. Personnel for the Anti-Money Laundering Department

The personnel of the Compliance & Anti-Money Laundering Department expressly assigned to the Anti-Money Laundering Department must be adequate in terms of number, technical and professional skills, and updating, also through the provision of continuous training sessions. In order to ensure across-the-board skills and to acquire an overall and integrated view of the control activities carried out by the Anti-Money Laundering Department, the Bank periodically evaluates the composition of the human resources in terms of qualifications and number.

3.6 Coordination with other Control Departments

3.6.1 Risk Management

The Anti-Money Laundering Department collaborates with the Risk Management Department in order to manage the risk of money laundering and terrorist financing within the Risk Appetite Framework (RAF).

3.6.2 Internal Audit[18]

The Internal Audit Department of the Bank verifies the degree of adequacy of the corporate organisational structure and its compliance with current legislation, and also monitors the functionality of the overall internal control system.

[18] Chapter II, Section III, Provision on AML Department.