REGULATIONS ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Latest update: 6 July 2021

Contents

1. INTRODUCTION 3
1.1 Purpose *3*
1.2 Scope of application and procedures for adoption *3*
1.3 Summary of updates *4*
2. GENERAL PRINCIPLES 5
2.1 Assessment of the exposure to the risk of money-laundering and terrorist financing *6*
2.2 Due Diligence and Know Your Customer activities *7*
2.2.1 Verification of the data and information collected *8*
2.2.2 Due diligence by third parties or on behalf of third parties *9*
2.2.3 Due diligence in the event of remote operations *9*
2.2.4 Simplified due diligence *9*
2.2.5 Enhanced due diligence *10*
2.3 Risk profile and monitoring on an ongoing basis *11*
2.4 Reporting suspicious transactions *12*
2.4.1 Reporting obligations on transfers of cash and bearer securities *13*
2.5 Data retention and registration *13*
2.6 Personnel training *14*
3. ROLES AND RESPONSIBILITIES 15
3.1 Parent Company *15*
3.1.1 Board of Directors *15*
3.1.2 Chief Executive Officer *16*
3.1.3 Board of Statutory Auditors *17*
3.1.4 Supervisory Body pursuant to Italian Legislative Decree No. 231/01 ..... *18*
3.1.5 Head of the Group's Anti-Money Laundering function *18*
3.1.6 Manager in charge of suspicious transaction reporting *18*
3.2 Companies belonging to the Group *20*
3.3 Corporate functions *20*
3.3.1 Anti-Money Laundering function *20*
3.3.2 Internal audit function *22*
3.3.3 Contact or support structures for transactions with customers and counterparties *22*

1. Introduction

1.1 Purpose

The Regulations illustrate and justify the choices made by the Banco BPM Group to prevent the risks of involvement in money laundering and financing of international terrorism.

1.2 Scope of application and procedures for adoption

The Regulations apply:

- to the financial intermediaries belonging to the Group with registered offices in Italy (subject to the anti-money laundering provisions as per Italian Legislative Decree No. 231/07);
- to other parties carrying out financial activities belonging to the Group with registered offices in Italy (subject to the anti-money laundering provisions as per Italian Legislative Decree No. 231/07).

Moreover, although they are not subject to the provisions on prevention of money laundering and terrorist financing as per Italian Legislative Decree No. 231/07, and in order to facilitate the application of the measures envisaged by Italian Legislative Decree No. 109/07, as amended and added to, the Regulations apply:

- to all the other Group Companies with registered offices in Italy, limited to the principles of full knowledge of their respective counterparties;
- to the Banks belonging to the Banking Group based abroad, in compliance and compatibly with current local laws and regulations, for the strengthening of organisational controls in the area of the prevention of money laundering and terrorist financing, to allow the assessment of the specific risk exposure also during the Group's internal assessment.

Following approval by the Board of Directors of the Parent Company, the Regulations and their subsequent amendments shall be implemented by the relevant Management Bodies of the Subsidiaries.

1.3 Summary of updates

Progressive	Date of update	Summary content update
Initial approval	30/01/2017	
1st update	29/09/2020	Appointment of the Group Anti-Money Laundering Manager as the first person delegated to report suspicious transactions and to notify infringements to the competent Authorities, replacing the Compliance Manager (see resolution of the Board of Directors of Banco BPM dated 29 September 2020).
2nd update	06/07/2021	Updating of the Regulations to bring them in line with the Bank of Italy Instructions requiring the Body with strategic supervisory functions to approve a policy explaining and justifying the choices made by the Group on the different significant aspects concerning organisational structures, procedures and internal controls, due diligence and data retention, consistent with the principle of proportionality and effective exposure to money laundering risk.

2. General Principles

Sector regulations aim at ensuring the efficiency of the markets, the promotion of competition, fair conduct, the respectability of company representatives, the transparency of ownership structures and relations with customers and the effectiveness of the organisational structure and internal controls, contributing to preventing the use of the financial markets for money laundering [1]and terrorist financing.[2]

Laws and regulations provide for intermediaries to have resources, procedures and organisational functions that are clearly identified and suitably specialised. More specifically, they require:

- the adoption of suitable strategies, policies, procedures and processes to identify, measure, assess and monitor the risk of money laundering, as well as measures to prevent the risk to which they are exposed;
- the accountability of employees and external staff;
- the clear definition, at the various levels, of roles, duties and responsibilities, as well as the specification of procedures ensuring compliance with the obligations of customer due

[1]Money-laundering*:* the following acts, if intentionally committed, represent money laundering:

- converting or transferring assets, carried out in the knowledge that they originate from criminal activity or participation in such activity, for the purpose of concealing or disguising the unlawful origin of the assets or assisting anyone involved in this activity in avoiding the legal consequences of their actions;
- concealing or disguising the true nature, origin, location, use, movement or ownership of the assets or the rights thereto, carried out in the knowledge that those assets originate from criminal activity or participation in such activity;
- purchasing, holding or using assets in the knowledge that, at the time of their receipt, those assets originate from criminal activity or participation in such activity;
- participating in one of the acts indicated above, associating for the purpose of committing such acts, attempting to perpetrate such act, assisting, instigating or advising someone to commit the act or facilitating its execution.

The act is considered money laundering even if the activities that generated the assets to be laundered are carried out in the territory of another EU Member State or a third country.

[2] Terrorist financing: any activity, using any means, for the purpose of collecting, financing, brokering, storing, holding in custody or disbursing funds or economic resources, realised in any manner, which are to be fully or partly used for the purpose of committing or favouring the commission of one or more terrorism-related offence as envisaged by the Italian Criminal Code, irrespective of whether the funds or economic resources are actually used in committing said offences.

diligence[3] and suspicious transaction reporting, [4]retention of documentation and records of relationships[5] and transactions[6];

- the set-up of a special function in charge of overseeing the activities for the prevention and management of money-laundering and terrorist financing risk;
- a system of Corporate Control Units (hereinafter CCU), the components of which are coordinated, also through suitable information flows, and which is, at the same time, consistent with the articulation of the structure, the complexity, the size of the company, the type of services and products offered and the extent of risk that may be associated with the characteristics of its customers;
- a control activity that aims at ensuring that staff and external staff comply with internal procedures and all regulatory obligations, notably in regard to active cooperation and ongoing review of customers' operations, to communication and reporting obligations and the safeguarding of confidentiality in the reporting process.

The Group has sought to respond to the complexity and danger of the phenomenon in a responsible and dedicated manner, paying particular attention to the quality and continuous improvement of the instruments for preventing and combating money laundering and terrorist financing, extending them also to those areas not directly envisaged through a full knowledge of the counterparty.

2.1 Assessment of the exposure to the risk of money-laundering and terrorist financing

The assessment of the Group's exposure to the risk of money-laundering and terrorist financing is carried out by the AML function through an internal assessment, which also involves the individual subsidiaries, therefore providing an integrated assessment of the risk exposure of the entire Group.

The internal assessment is carried out at least once a year; it is also performed whenever major new risks arise or whenever there are significant changes in the existing risks, in the operations or in the organisational or corporate structure of the Bank and the Group. The

---

[3] Customer due diligence consists of identifying and verifying the identity of the customer, the executing party (if any) and the beneficial owner (if any), obtaining information on the purpose and intended nature of the ongoing relationship and the occasional transaction, and carrying out constant monitoring during the course of the ongoing relationship.

[4] Suspicious transaction: a transaction which, due to objective connotations (deduced from the characteristics, entity, nature of the transactions) or subjective connotations (deduced from the knowledge of circumstances, in view of the functions performed, also taking into account the economic capacity and the activity carried out by the party to whom it relates), leads, on the basis of the elements available to the reporting party, acquired as part of the activities carried out, to the belief that the funds used may be of unlawful origin or intended for terrorist financing.

[5]Ongoing relationship: long-term relationship which is part of the performance of institutional activities by financial intermediaries and other parties conducting financial activities, results in multiple transactions of deposit, withdrawal or transfer of means of payment and does not end after a single transaction.

[6] Transaction: the transmission or handling of means of payment or the performance of legal acts involving assets.

internal assessment is carried out using a methodology that values the relevant business lines and allows the segmentation of customers into classes characterised by similar needs, expectations and behaviour.

The identification of the level of inherent risk - as identified through the valuation of typical or exceptional risk factors (operations, products and services, customers, distribution channels, geographic area and countries of operation) - is followed by an analysis of the vulnerability of the safeguards and by the verification, in this context, of the quality of the information flows to the corporate bodies as well as of every regulatory, process and safeguard aspect connected to them. For the purposes of the inherent risk assessment, the Bank does not promote business proposals involving cryptocurrencies.

The combination of the inherent risk and vulnerability ratings for each business line determines the assignment of the residual risk category associated with each business line and the consequent identification of remedial and mitigating actions. The overall residual risk level is then given by the residual risk values of the individual business lines identified, weighted by the weight assigned to each line.

The remedial actions identified are proposed by the Chief Executive Officer as part of the Annual Report prepared by the AML function and approved by the Board of Directors.

The AML function coordinates and monitors the implementation of the remedial actions identified and verifies, on an ongoing basis, that these are able to ensure the adequate prevention and mitigation of the risks to which the Group is effectively exposed.

2.2 Due Diligence and Know Your Customer activities

Due Diligence and Know Your Customer activities are the cornerstone of the prevention of the risk of money laundering and terrorist financing and must be aimed at the prior identification and analysis of all information useful for assessing the potential risk associated with the execution of the transaction or the opening of the account, as well as the activation of the relationship under review.

Due diligence activities must be carried out, in the way described in the provisions and instructions issued by the Supervisory Authority, at least at the time of the establishment of an ongoing relationship, the execution of an occasional transaction, the occurrence of doubts as to the correctness of the information in the system as well as in the presence of elements arousing suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold that may apply.

Following the risk-based approach, the organisational model envisages the use of a questionnaire, the contents of which are articulated according to the specific level of risk, taking also into account the nature and purpose of the relationship or occasional transaction.

In any event, in addition to the conduct of the customer and the nature of the transaction or relationship, the following are deemed to be important: the risk elements linked to the specific characteristics of the customer, the beneficial owner, the executing party or the counterparty and the relations between them, the type of service or product requested or offered, as well as the countries or specific features of the geographical areas involved (EU countries and third

countries with effective money laundering prevention systems, or third countries believed to lack effective money laundering prevention systems or believed to have a high level of corruption, subject to sanctions, embargoes or similar measures).

The inability to fully comply with customer due diligence requirements leads to the inability to establish the ongoing relationship or to execute the transaction or, in the case of an existing ongoing relationship, the inability to continue it. In all these cases, the filing of a suspicious transaction report should be considered.

2.2.1 Verification of the data and information collected

For customers who are natural persons and executing parties the identity shall be verified by checking the authenticity and validity of the identity document or other equivalent identification document and, for executing parties, the existence and extent of the power of representation. For customers other than natural persons, the identification data shall be verified through the query, independently or through the customer, of reliable and independent sources, the results of which shall be stored in hard copy or electronic form.

If a customer or counterparty is not a natural person, not only the executing party, but also the beneficial owner must always be identified, according to the principles of reasonableness set out in the operating rules. The information and documentary set collected for customers other than natural persons, necessary for the fulfilment of the due diligence obligations also in regard to the full identification of the beneficial owner, must be proportional to the complexity of the investment chain, the specificity of the legal form used, any irregularity indicators which should include the riskiness of the economic sector in which the customers operates.

The information acquired when identifying the customer, the executing party (if any) and the beneficial owner is verified on the basis of documents, data or information obtained from a reliable and independent source, also using automated control procedures integrated with public sources. In particular, the fulfilment of the due diligence obligations includes checking whether the identified parties are on any AML watchlists. Watchlists also include the lists of persons and entities associated with terrorist financing adopted by the European Commission. The external lists are managed and maintained by independent providers. The lists make it possible to structure the operational blocks necessary to guarantee the extension of the investigations for a complete assessment of the risk of money-laundering or terrorist financing.

These activities, together with monitoring activities, make it possible to continuously monitor the money laundering risk associated with specific transactions.

Similar measures are also taken with regard to counterparties, even though these are not the direct recipients of the regulatory obligations, in order to ensure that they are fully aware of them.

2.2.2 Due diligence by third parties or on behalf of third parties

Fulfilment of due diligence obligations by or on behalf of third parties occurs in the case of distribution agreements, or in the case of impromptu requests. The questionnaire in which the information is summarised for due diligence purposes is formally shared between the parties.

The operational provisions distinguish between third parties allowed to carry out all stages of due diligence and third parties that are only allowed to carry out the identification of the customer, the executing party and the beneficial owner.

The use of shell banks, or the use of information provided only by intermediaries based in high-risk third countries, is prohibited in any case.

2.2.3 Due diligence in the event of remote operations

Particular attention is paid to remote operations, i.e. operations carried out in the absence of the customer or the executing party, given the risks associated with the absence of direct contact and the risk of fraud, including identity theft.

In order to ensure that the risks associated with remote transactions are properly controlled, a strengthening of the safeguards is envisaged both at the time of identification of the customer, executing party and beneficial owner and when monitoring their transactions. These safeguards are to be considered dynamic, since they have to be adapted to the continuous technological developments or to the specific risks related to this type of transaction, as also assessed in the internal assessment carried out by the AML function.

In the event of remote identification, copies of two valid identity documents must be obtained, a transfer must be made from a bank account in the same name opened with another intermediary in Italy or in an EU country, and the data and information acquired must be checked against an external database in order to detect any irregularities.

Where no anomalous or suspicious elements are identified, the relationship is established. If, on the other hand, irregularities are identified, further investigation is required in line with the level of risk identified, which may include completing the identification with a face-to-face meeting.

The identification of the customer that is a natural person can be carried out online remotely following a registration procedure based on technological solutions provided by external operators and recognised by the market. Remote video-identification solutions are subject to prior assessment by the Anti-Money Laundering function to verify their compliance with the operating instructions of the Supervisory Authority.

2.2.4 Simplified due diligence

If the risk of money laundering and terrorist financing is low, due diligence requirements are simplified, reducing the scope and frequency of the related obligations. The model adopted envisages the collection of a due diligence questionnaire, which provides a set of information that is differentiated from the one collected in the ordinary due diligence process. For

customers other than natural persons, the beneficial owners and the executing party of occasional transactions must be identified.

The customer is in any case under regular monitoring during the course of the ongoing relationship, to verify that the low-risk factors that led to the application of simplified due diligence continue to be present.

2.2.5 Enhanced due diligence

If the risk of money laundering and terrorist financing is high, due diligence requirements are enhanced by extending the scope and frequency of the related obligations.

The model adopted envisages the collection of a due diligence questionnaire, which provides a set of information that is differentiated from the one collected in the ordinary due diligence process. In particular, enhanced due diligence involves the collection of additional information on the customer and the beneficial owner, a more accurate assessment of the nature and purpose of the relationship, the intensification of the frequency of checks and more in-depth analysis carried out as part of the constant monitoring of the ongoing relationship.

The intensification of the frequency of checks and greater depth of analysis in the context of the control activities on the ongoing relationship is also envisaged. Due diligence is carried out by the units which have the relationship with the customer, possibly supported by the AML function.

The enhanced due diligence measures are applied, in any case, in the following cases, which are believed to present a higher risk of money laundering:

- ongoing relationships or occasional transactions with customers and beneficial owners who are politically exposed persons (PEPs), which require: (i) authorisation of the initiation or continuation of the relationship or the execution of the occasional transaction by a senior manager[7]; (ii) an assessment by the AML function prior to authorisation in all cases where the PEP has a significant anti-money laundering record; (iii) a more thorough examination of the elements relating to the customer and the persons connected by family or business ties, the beneficial owners, the purpose and nature of the relationship or transaction, the origin of the funds used or their intended use, and the relationship between the parties involved.

  For PEPs for whom anti-money laundering records are found, the qualification and application of enhanced due diligence measures are extended up to three years after leaving the public office.

- customers belonging to business categories which, by virtue of their characteristics or their operations in specific business sectors, present a higher risk of money laundering;

[7] The Chief Executive Officer of the Parent Company delegates powers to personnel within the bank's workforce, who are provided with a sufficient level of autonomy to make decisions affecting this level of risk. These personnel must hold senior positions in central corporate units or Area Divisions. In the case of Subsidiaries, authorisation power remains with the party holding powers of administration or management, with the right to delegate, only in cases of temporary impossibility, in favour of a member of their staff or to another party exercising equivalent functions.

- relationships and transactions involving high-risk third countries, with the obligation to refrain from establishing or continuing relationships or carrying out transactions to which fiduciary companies, trusts, limited companies (or those controlled through bearer shares) based in high-risk third countries are directly or indirectly a party;
- cross-border correspondent banking relationships with a credit or financial institution in a third country, with the requirement to collect a set of mandatory documents articulated in regard to the registered office of the counterparty, the parent company or the beneficial owner, to be able to assess the soundness of the controls in place to prevent the risk of money laundering and terrorist financing, as well as the potential exposure in terms of reputational risk.

Second-level controls on cryptocurrency transactions are carried out by the Anti-Money Laundering function, also by using remote indicators.

Relationships and transactions involving counterparties or third countries subject to restrictions in terms of financial sanctions and embargoes are monitored by laying out Guidelines also aimed at specifying prohibitions, limitations and blocks.

2.3 Risk profile and monitoring on an ongoing basis

The monitoring of customer transactions ensures, on an ongoing basis, the identification of elements that may also lead to the adoption of enhanced due diligence measures.

The assignment of the risk profile is mainly based on the adoption of automated processes which take into account, among other things, evidence from anti-money laundering lists[8] and the customer's relationships with related parties, the provisions of which are specified and periodically reviewed by the AML function.

The model of harmonisation of the risk profile assigned to the customer prudentially guarantees, at Group level, the application of the safeguards provided for by the highest risk band.

According to the risk-based approach, four risk bands are identified, which are updated at different frequencies: i) high risk, at least every 12 months; ii) medium risk, at least every 24 months; iii) low risk, at least every 48 months and iv) immaterial risk, at least every 96 months.

Without prejudice to the need to update the risk profile of high-risk customers at least every 12 months, the Subsidiaries, also on account of specific business and customer characteristics, may update the risk profile with frequencies different from those indicated above.

When the risk profile is updated, in-depth analyses are articulated according to criteria of proportionality, accuracy and adequacy, diversifying their extension, depth and frequency according to the specific level of risk and any increase in this.

[8] Such as the PEP list, which lists individuals classified as Politically Exposed Persons, or the Justice Insights list.

If the customer's risk profile worsens, with a move into the high-risk band, the profile expires immediately and enhanced due diligence must be performed; a deterioration in the risk profile results in the assignment of an earlier due date than the existing one.

For entities with a low and insignificant risk profile, the update of the due diligence may also be performed automatically.

The update is always due when the analysis of the customer's position shows that information previously acquired and used in the course of due diligence may no longer be current.

The power to manually adjust the risk profile pertains to the AML function alone.

Control activities may also be carried out using transaction monitoring tools, i.e. event-based checks aimed at identifying significant risk situations.

Finally, the model adopted envisages specific controls and provisions for the management and monitoring of transactions which, due to objective characteristics, present a higher risk of money-laundering or terrorist financing, having taken into account the results of the internal assessment, the National Risk Assessment and the elements brought to the attention of intermediaries by the Supervisory Authority, notably in regard to the exposure to the risk of the third country where the funds used originate.

2.4 Reporting suspicious transactions

The head of the unit handling the customer relationship must promptly report to the AML function when there is suspicion or reasonable grounds to suspect that money-laundering or terrorist financing activities are being or have been carried out or attempted, or that the funds, regardless of their amount, originate from the commission of criminal activity. The obligation extends to all personnel who, in regard to the activity carried out, have reason to suspect that a customer transaction is carried out for money-laundering or terrorist financing purposes.

To ensure prompt reporting and uniformity of conduct, computerised procedures highlight transactions that are anomalous in terms of frequency or amount, or in terms of destination or origin of the funds, and support the assessments carried out by personnel on their own initiative.

The AML function reviews the reports received and, if it finds them well-founded in light of all the information at its disposal and of any other information acquired also from open sources, forwards them to the Financial Intelligence Unit (FIU), omitting the name of the reporting party. If, on the other hand, the AML function does not find sufficient elements of suspected transactions to justify alerting the FIU, it keeps records of the assessments made, the information and the documents considered.

In the case of customers that have been repeatedly reported, controls are strengthened and upper-level management may be involved in assessing whether to maintain or terminate the relationship

If the AML function becomes aware of suspected money-laundering or terrorist financing transactions arranged by the customer but not yet executed and for which a possible seizure

order seems likely, it promptly intervenes with the FIU to investigate the situation and request the issuance of an order to suspend the suspicious transactions.

The AML function responds promptly to requests for further investigation or information received from the FIU or the judicial authorities.

All appropriate measures are taken to maintain the confidentiality of the identity of the persons involved in the reporting of suspicious transactions. The reporting party may only be disclosed when the judicial authorities, by justified decree, consider it essential for the purposes of ascertaining the offences for which proceedings have been initiated.

It is forbidden to inform the client concerned or third parties that a report has been made, that further information has been requested by the FIU or that investigations or in-depth studies on money-laundering or terrorist financing have been or might be carried out.

The names of customers for which suspicious transactions have been reported can only be viewed in the manner and in the cases regulated within the corporate operational processes, given the importance that such information might have when initiating new contractual relationships or evaluating the operations of existing customers, such as requests for credit facilities.

The risk profile of the reported customers remains high until the lapse of a period of time suitable for considering the original risk as having been mitigated, also due to the absence of further causes for suspicion or requests for further investigation by the FIU. In any case, when the FIU informs the customer that the report of a suspicious transaction has been closed, a score is assigned.

2.4.1 Reporting obligations on transfers of cash and bearer securities

Banco BPM ensures centralised reporting to the MEF of breaches of restrictions on cash and bearer securities of which it becomes aware, according to the time limits and procedures envisaged in the relevant laws and regulations.

It also prohibits the opening, in any form, of accounts and savings passbooks anonymously or in fictitious names.

2.5 Data retention and registration

To store customer data and information, the Archivio Unico Informatico - AUI (a centralised computer archive) is used as a standardised archive and as a suitable tool to ensure accessibility by the Supervisory Authority, integrity, transparency, inalterability and data logging of documents, data and information. Specific procedures are in place to ensure the completeness of the records and their controlled cancellation, if any.

The data and information are acquired during the due diligence on the customer, the executing party and the beneficial owner and are kept for a period of ten years from the termination of the ongoing relationship or the execution of the occasional transaction. With regard to occasional transactions that do not require due diligence, data and information uniquely identifying the customer and the executing party are retained for the same period.

The model adopted is based on compliance with the applicable data protection provisions and ensures the retention of information relating to transactions, including those involving amounts below the threshold for storage in the AUI.

The data is aggregated according to the criteria specified by the FIU in order to send the Aggregated AML Reports on a monthly basis. Suitable procedures are also specified to send to the Supervisory Authority the aggregated reports on the use of cash (Objective Communications).

2.6 Personnel training

Personnel training is carried out continuously and systematically, taking into account regulatory developments and the anti-money laundering model adopted, and includes a final report on the results of the activities carried out.

An annual training plan is laid out with the aim of continuously updating all personnel in line with regulatory developments and providing specialised training for specific needs linked to the roles and responsibilities of the personnel involved.

The tools and methods adopted (such as classroom training, remote learning or virtual classrooms) are specified according to the purpose of the courses to be delivered.

The monitoring of the training activities covers not only the contents but also the level of effectiveness of the courses provided, through an initial check on the level of knowledge of the personnel involved and a final test aimed at assessing the level of learning after the course provided.

The didactic material is made available to the personnel involved in the training course on a durable medium and with easy access for consultation.

3. Roles and Responsibilities

According to Banco BPM Group's organisational model for the prevention and mitigation of the risk of money laundering and terrorist financing, the following are involved:

- the Board of Directors, the Chief Executive Officer and the Board of Statutory Auditors of the Parent Bank;
- the corporate bodies of financial intermediaries, as well as other Group financial operators based in Italy, other Group companies based in Italy other than those mentioned above and Group companies based in foreign countries;
- the Head of the Group's Anti-Money Laundering function;
- the Anti-Money Laundering function;
- the Manager in charge of suspicious transaction reporting (known as "STR Officer");
- the internal audit function;
- the contact or support structures for relations with customers and counterparties.

In addition, the Banco BPM Group has adopted a centralised model, whereby the subsidiaries subject to the reference regulations have outsourced the anti-money laundering function to the Parent Bank's Anti-Money Laundering function and have identified specific anti-money laundering contact persons.

Lastly, Banco BPM has set up an integrated Internal Control System, involving the CCUs and, among them, Anti-Money Laundering function.

3.1 Parent Company

Strategic guidelines on money laundering risk management and anti-money laundering controls are adopted by the Parent Company's corporate bodies.

3.1.1 Board of Directors

The Board of Directors, as the body with strategic supervisory functions:

- approves and periodically reviews the strategic guidelines and governance policies for risks relating to money laundering and the terrorist financing, for the purpose of ensuring, in line with the risk-based approach, the suitability with respect to the entity and type of risks that the Banco BPM Group’s activities are effectively exposed to, as described in the internal risk assessment document;
- approves the Regulations on the prevention of money laundering and terrorist financing, which describes and justify the choices made by the Banco BPM Group on the different significant aspects concerning organisational structures, procedures and internal controls, due diligence and data retention, consistent with the principle of proportionality and effective exposure to money laundering risk.

- identifies AML tasks and responsibilities, as well as formalities for coordination and cooperation with other CCUs;
- approves the guidelines of an organic, coordinated system of internal controls, which ensures the prompt detection and management of money laundering and terrorist financing risk and ensures its effectiveness over time;
- approves the principles for handling relations with customers classified as "high-risk";
- appoints, after consulting the Board of Statutory Auditors, the Head of the Anti-Money Laundering function, upon the proposal of the Internal Control, Risks and Sustainability Committee, supported by the Appointments Committee, and revokes this, after consulting the Board of Statutory Auditors, after hearing the opinion of the Internal Control, Risks and Sustainability Committee, supported by the Appointments Committee;
- ensures, on an ongoing basis, that the roles and responsibilities for the activity against money laundering and terrorist financing are specified and assigned clearly and appropriately, guaranteeing that operational and control units are separated and that these units are equipped with adequate resources in terms of quality and quantity;
- ensures that an adequate, complete and timely system of information flows is in place in regard to the Corporate Bodies ("*vertical flows*") and between control functions ("*horizontal flows*");
- ensures confidentiality is maintained within the suspicious transaction reporting procedure;
- reviews, at least once a year, the reports on the activities carried out by the AML function, as well as the report on the results of the internal assessment of money-laundering risks;
- ensures that the deficiencies and anomalies detected as a result of the different control levels are promptly brought to its attention and furthers the adoption of appropriate corrective measures, the effectiveness of which it assesses;
- assesses the risks arising from transactions with third countries associated with higher money laundering risks, identifying the safeguards to mitigate them and monitoring their effectiveness.

3.1.2 Chief Executive Officer

The Chief Executive Officer, as the body with management functions, through the relevant functions:

- oversees the implementation of the strategic guidelines and money-laundering risk management policies approved by the Board of Directors and is responsible for adopting all the measures necessary to ensure the effectiveness of the organisation and the system of anti-money laundering controls, taking into account, when preparing operating procedures, the indications and guidelines issued by the relevant authorities and international bodies;
- specifies and oversees the implementation of a system of internal controls for the prompt detection and management of money laundering risk and ensures its effectiveness over time, according to the results of the internal risk assessment;

- ensures that operating procedures and information systems allow for the proper fulfilment of customer due diligence and documents and information retention obligations;
- with regard to the reporting of suspicious transactions, specifies and oversees the implementation of a procedure, suited to the specific business characteristics, size and complexity of the bank, that can ensure certainty of reference, uniformity of conduct, generalised application to the entire structure, full use of relevant information and traceability of the assessment process;
- adopts measures aimed at ensuring compliance with the confidentiality requirements of the suspicious transaction reporting procedure, as well as tools, including IT tools, for detecting anomalous transactions;
- specifies and sees to the implementation of the initiatives and procedures necessary to ensure the timely fulfilment of the reporting obligations to the Authorities envisaged by the legislation on prevention of money laundering and terrorist financing activities;
- specifies the Regulations on the prevention of money laundering and terrorist financing, submitted for the approval of the Board of Directors, and oversees their implementation;
- specifies and oversees the implementation of information procedures aimed at ensuring that all the corporate units involved and the bodies entrusted with control functions are aware of the risk factors;
- specifies and oversees the implementation of procedures for handling relations with customers classified as "high-risk", according to the guidelines laid down by the Board of Directors;
- decides on personnel training and education programmes on the obligations arising from regulations on the prevention of money laundering and terrorist financing, ensuring the continuity and systematic nature of training activities, also taking into account developments in the reference regulations and the procedures specified and adopted by the bank;
- decides on the instruments to be used to verify the activity carried out by employees and external staff in order to detect any anomalies arising, specifically, in conduct, in the quality of communications addressed to the contact persons and corporate units as well as in the relationships of employees or external staff with customers;
- ensures, in cases of remote operations, the adoption of specific IT procedures to ensure compliance with regulations on the prevention of money laundering and terrorist financing, with particular reference to the automatic detection of anomalous transactions.

3.1.3 Board of Statutory Auditors

The **Board of Statutory Auditors**, in its capacity as a supervisory body, monitors compliance with laws and regulations and the completeness, functionality and adequacy of the control systems for the prevention of money laundering and terrorist financing. In exercising its powers, the Board of Statutory Auditors makes use of the internal structures to carry out the necessary checks and verifications and uses information flows from other corporate Bodies, from the Head of the Anti-Money Laundering function and from other CCUs.

In this context, the Board of Statutory Auditors:

- assesses the suitability of procedures for customer due diligence, the retention of information and the reporting of suspicious transactions;
- analyses the reasons for deficiencies, anomalies and irregularities detected and promotes the adoption of suitable corrective measures;
- is consulted during the procedures for appointing and dismissing the Group Anti-Money Laundering Manager and the Manager in charge of suspicious transaction reporting, and during the definition of the elements of the overall architecture of the system for managing and controlling the risk of money laundering and terrorist financing.

The members of the Board of Statutory Auditors shall inform the Supervisory Authority without delay of all facts of which they become aware in the performance of their duties, which may represent serious or repeated or systematic or multiple violations of the applicable provisions of law and of the related implementing provisions.

3.1.4 Supervisory Body pursuant to Italian Legislative Decree No. 231/01

The Parent Company's Supervisory Body and the Supervisory Bodies referred to in Italian Legislative Decree No. 231/01 (or the Bodies with control functions performing the functions of the latter) of Group Companies oversee the functioning and observance of the Organisation, management and control model pursuant to Italian Legislative Decree No. 231/01.

The Supervisory Body informs the Supervisory Authorities without delay of all facts or actions that it becomes aware of that may represent a breach of the implementing provisions of said decree. The reports may be made jointly with other corporate bodies or functions.

The Supervisory Body receives information flows from corporate units and may access, without limitation, any relevant information for the purpose of carrying out its duties.

3.1.5 Head of the Group's Anti-Money Laundering function

The Head of the Group's Anti-Money Laundering function must comply with suitable independence, authority and professional competence requirements.

They are included among the heads of CCUs and have no direct responsibility over operational areas subject to control; they must not have direct responsibilities over operating areas subject to control, nor report to the persons in charge of said areas;

The Head of the Group's Anti-Money Laundering reports directly, without restriction or intermediation, to the corporate bodies of the Bank and its subsidiaries, including the 231/01 Supervisory Bodies where they have been set up.

3.1.6 Manager in charge of suspicious transaction reporting

The legal representatives of financial intermediaries and other parties that carry out financial activities of the Group may grant a delegate the powers to assess and send reports of suspicious transactions, subject to the resolution of the body with strategic supervision responsibility, having consulted the control body.

In line with the anti-money laundering and terrorist financing risk oversight model adopted at Group level, the Parent Company:

- names the Head of Anti-Money Laundering of the Parent Company as the first delegate in charge of assessing the suspicious transaction reports that are received from any Banco BPM organisational structure (central and peripheral). In the event of absence or impediment of the first delegate, this shall be replaced by other delegates identified within the Anti-Money Laundering function of the Parent Company;
- proposes to the legal representatives of the other Group companies that have outsourced the anti-money laundering function and intend to appoint a delegate, to assign the position of first delegate to said Head of the Anti-Money Laundering function of the Parent Company and to other delegates identified as substitutes, in the event of absence or impediment of this, within the Anti-Money Laundering structure of the Parent Company.

The delegate in charge of suspicious transaction reporting is responsible for:

- assessing the suspicious transactions reported by the head of the structure which actually manages relations with customers ("first level") and those of which he/she has otherwise become aware in the course of his/her activities. In this connection, he/she acquires all relevant information, either directly or through the structures identified on a case-by-case basis at the intermediaries or other parties that carry out financial activities of the Group.
- assessing, in the light of all available information, the suspicious transactions and transmitting to the FIU the reports considered well-founded, omitting the names of the persons involved in the transaction reporting procedure;
- keeping evidence of the assessments made within the procedure, even in those cases where a report to the FIU is not sent out.

The delegate has free access to information flows intended for the corporate bodies and structures involved in different roles, in managing and combating money laundering and terrorist financing. The delegate also acts as liaison with the FIU and promptly replies to any requests for further information received from this.

Without prejudice to the confidentiality of the identity of the first-level party that made the report, the delegate in charge of suspicious transaction reporting may allow the names made in the suspicious transaction report to be consulted - also using suitable IT databases - by the managers of the different operational structures of the Group, given the particular importance that such information may have when entering into new contractual relationships or assessing transactions of customers already acquired and the counterparties.

Intermediaries or other parties carrying out financial activities of the Group that have not assigned a mandate shall deliver to the delegate a copy of the reports sent to the FIU, or archived, including the reason for such decision. This delivery must be made using methods that guarantee the utmost confidentiality regarding the identity of the first-level manager that made the report. For the purpose of in-depth investigation of the irregular transactions and relationships within the entire Group, the delegate may use each and every structure of the subsidiaries, even those which have not granted the mandate.

3.2 Companies belonging to the Group

The Corporate Bodies of the Group Companies are aware of the choices made by the Parent Company and are responsible, each according to their own expertise, for the implementation, within their respective entity, of the strategies and policies specified on the subject of preventing the risks of involvement in money laundering and international terrorist financing.

In regard to the centralised model, through which all subsidiaries subject to the regulations outsource their activities to the Parent Company's Anti-Money Laundering function, contact persons are appointed, according to the Integrated Internal Control System Regulations, who functionally report to and support the Parent Company's Anti-Money Laundering function. The contact persons:

- have no direct responsibility over operational areas subject to control, nor are hierarchically subordinate to the heads of these;
- have direct access, together with the Group Anti-Money Laundering Manager, to the Bank's or Company's corporate bodies and are informed of corporate events concerning aspects falling within the Anti-Money Laundering remit, including communications received from the Supervisory Authorities;
- have direct access to all activities, including those outsourced, to verify their compliance with anti-money laundering regulations;
- collaborate in drawing up plans for the pertinent control activities, set out in the Annual Reports, to be submitted to the Board of Directors of the Parent Company and of the Bank or Company.

The foreign subsidiary Banca Aletti & C. (Suisse) S.A. must set up, within its regulatory compliance unit, a structure to prevent the risk of money laundering and terrorist financing. The Head of Regulatory Compliance, together with General Management, is responsible for information flows to local Supervisory Authorities. The Company carries out its activities according to the regulations of its own country and specifies with the Parent Company's Anti-Money Laundering function information flows for risk assessment purposes to ensure the risk is suitably assessed in the annual internal assessment.

3.3 Corporate functions

3.3.1 Anti-Money Laundering function

The Anti-Money Laundering function of the Parent Company is the CCU in charge of overseeing, for the Parent Company and the Group Companies that have outsourced the service, the processes for the prevention of money laundering and terrorist financing in the Group.

Pursuant to the supervisory provisions, the AML function is guaranteed the necessary independence. The AML function is given adequate economic resources, personnel and skills as needed to perform its tasks and has access to all company data as well as any information relevant to perform its role appropriately; the personnel must be adequate in number, technical and professional skills and their professional development must be ensured, also through ongoing training programmes.

AML personnel must not be involved in activities that the structures themselves are called upon to control.

The remuneration criteria for the manager and the personnel of the AML structures comply with the current legislation on remuneration policies and are consistent with the purposes of the function performed.

The Anti-Money Laundering structures, which report to the Group Anti-Money Laundering Manager, are responsible for:

- collaborating in defining the money-laundering risk management policies and the different stages of the process for managing this risk;
- collaborating in the definition of the system of internal controls and procedures aimed at preventing and combating money laundering risks and identifying the factors to be taken into account in assessing the risk of the persons assessed;
- identifying the applicable provisions and, with reference to these, verifying on an ongoing basis the adequacy of the process for managing money laundering risks and the suitability of the system of internal controls and procedures, and proposing organisational and procedural changes aimed at ensuring adequate supervision of money-laundering risks;
- defining the criteria and content of the information set required during due diligence in line with the evolution of money laundering and terrorist financing risks;
- conducting, in liaison with the manager in charge of suspicious transaction reporting, checks on the functionality of the reporting process and on the appropriateness of the assessments made by the first level on customer operations;
- conducting, in liaison with the other corporate functions concerned, the annual internal assessment on money laundering risks;
- performing a prior assessment of the money laundering risk associated with the offer of new products and services;
- verifying the reliability of the information system for the fulfilment of the obligations of customer due diligence, data retention and suspicious transaction reporting;
- transmitting to the FIU objective communications concerning transactions at risk of money laundering and, on a monthly basis, aggregate data concerning all transactions;
- preparing, in liaison with the other corporate units responsible for training, an adequate training plan aimed at ensuring continuous personnel development and participating, through direct involvement of its own resources, in teaching activities;
- preparing regular information flows for the corporate bodies and senior management and promptly informing them of any significant violations or deficiencies encountered;
- contributing to the preparation of the Integrated Report on the Internal Control System and expressing its assessment, based on the results of the checks carried out and on the knowledge of the company's areas of operation, insofar as it is concerned;

- at least once a year, preparing and submitting to the Corporate Bodies the Report on the activities carried out, describing the initiatives adopted, the issues detected, the corrective action to be undertaken and personnel training activities. The report also includes the results of the internal assessment on the money-laundering and terrorist financing risks and a summary of the regulations and supporting documents made available to all personnel.

3.3.2 Internal audit function

With regard to the prevention of money laundering and terrorist financing, the Parent Company's internal audit function verifies on an ongoing basis the suitability of the organisational set-up and its compliance with reference laws and regulations and supervises the operation of the internal control system as a whole.

Through systematic checks, including inspections, the internal audit function verifies:

- ongoing compliance with the due diligence obligation, both when entering into a relationship and throughout its development over time;
- the actual acquisition and organised storage of the data and documents required by regulations;
- the actual degree of involvement of employees and external staff as well as the managers of the central and peripheral structures in implementing the communication and reporting obligations.

Inspection activities, both remote and on-site, are planned to ensure that all peripheral and central operational structures are audited over a suitable time period and that the audits are more frequent for structures with greater exposure to the risk of money laundering and terrorist financing, as well as for customers with a high risk profile.

The internal audit function carries out follow-up activities to verify the adoption of the corrective measures for the deficiencies and irregularities detected, ensuring that these are suited to prevent similar situations to occur.

The internal audit function reports, at least once a year, to the corporate bodies on the activities carried out and their outcome, while maintaining confidentiality concerning reports of suspicious transactions.

3.3.3 Contact or support structures for transactions with customers and counterparties

The structures in contact with or supporting transactions with customers and counterparties provide the first-level control on the risk of money laundering and terrorist financing and, within the scope of their activities, are responsible for:

- carrying out due diligence / know-your-customer activities at the time of the establishment of the relationship with customers / activation of relationships with counterparties or execution of occasional transactions;

- providing adequate monitoring of transactions, in such a way as to allow the timely identification of any potentially suspicious transaction.

The controls carried out as part of the above activities are the subject of specific and precise provisions in the corporate procedures.