REGULATIONS ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Last update: **16 December 2025**

Contents

1 Introduction

1.1 Purpose

The Regulations illustrate and explain the choices that the Banco BPM Group adopts with regard to preventing the risks of involvement in money laundering, international terrorist financing and the proliferation of weapons of mass destruction, the financing of companies that produce anti-personnel mines, cluster munitions and submunitions, as well as non-compliance with national and European Union restrictive measures.

1.2 Scope of application and implementation procedures

The Regulations apply:

- to the financial intermediaries belonging to the Group with registered offices in Italy (subject to the anti-money laundering provisions of Italian Legislative Decree 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 of Italian Legislative Decree 231/07).

Moreover, despite their not being directly subject to the provisions on anti-money laundering, terrorist financing and the proliferation of weapons of mass destruction referred to in Italian Legislative Decree 231/07, also to facilitate the implementation of the measures provided for by Italian Legislative Decree 109/07, as subsequently amended and supplemented, and compliance with the prohibitions under Italian Law 220/2021, the Regulations apply:

- to all the other Group companies with registered offices in Italy, solely for the principles of full knowledge of their respective counterparties and compliance with the restrictive measures and with the prohibition under Italian Law 220/2021;
- to the parties exercising financial activities belonging to the Group with registered offices abroad, in compliance and compatibly with current local laws and regulations, to strengthen the organisational controls in the area of the prevention of money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as to comply with the restrictive measures and the prohibition under Italian Law 220/2021, and to allow the assessment of the specific risk exposure also during the Group's internal assessment.

The Regulations, along with their subsequent amendments, following approval by the Board of Directors of the Parent Company, are implemented by the relevant Management Bodies of the subsidiaries which resolve, insofar as they are responsible, on the implementation of the Regulations and guarantee that any internal Regulations are consistent with that of the Group.

1.3 Summary of updates

Sequence	Date of update	Update summary content
Initial approval	30/01/2017	
1st update	29/09/2020	Appointment of the Head of the Group Anti-Money Laundering Function 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	Regulations updated to bring them in line with the Bank of Italy Instructions requiring the Body with strategic supervisory functions to approve a policy describing and justifying the choices made by the Group on the different significant issues concerning organisational structures, procedures and internal controls, due diligence and data retention, in line with the criteria of proportionality and effective exposure to money laundering risk.
3rd update	22/07/2022	Formal changes to ensure the Regulations remain consistent with the Group's organisational structure.
4th update	12/05/2023	Update to regulate the relationship between Parent Company Anti-Money Laundering and the similar function of the Group companies that have not outsourced the activity in accordance with the Integrated Internal Control System Regulation (resolution of 8/05/2023).
5th update	07/11/2023	Update of the Regulations to adapt them to the changes made with the Bank of Italy Measure of 1 August 2023 on the organisation, procedures and internal controls to be applied for anti-money laundering purposes.
6th update	05/09/2024	Formal adjustments to implement (i) the reference to internal policies to govern the hypotheses of conflict of interest and (ii) the elimination of the option to use the audio/video recording procedure to identify a customer/natural person remotely for due diligence.
7th Update	27/03/2025	Update of the Regulations to extend the operational procedure already defined to authorise relations with politically exposed persons to customers residing or domiciled in high-risk countries, as well as to implement

		the obligations to assess the procedures used for the remote identification of customers.
8th update	16/12/2025	Update of the Regulations to adapt them to the new regulatory provisions that introduced as part of Italian Legislative Decree 231/07, the fight against the proliferation of weapons of mass destruction[1], compliance with the restrictive measures[2] and with the prohibition under Italian Law 220/2021[3].

[1] See art. 11 *"Urgent anti-money laundering measures"* of Italian Decree Law 95/2025 converted with amendments into Italian Law no. 118 (in Official Gazette no. 184, 9 August 2025)

[2] See note no. 48 of 8 April 2025 *"Implementation of the EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures"* (EBA/GL/2024/14)

[3] See *Instructions of the Bank of Italy, Covip, IVASS and MEF for exercising strengthened controls on the work of authorised intermediaries to counter the financing of companies producing anti-personnel mines, cluster ammunition and submunitions, in implementation of article 3, paragraph 1, of Italian Law no. 220 of 9 December 2021.*

2 General Principles

Sector rules seek to ensure the efficiency of the markets, the promotion of competition, proper conduct, the integrity of company representatives, the transparency of ownership structures and of customer relations, and the effectiveness of the organisational structure and of internal controls, by contributing to:

- hinder the use of financial mechanisms for money-laundering[4] and terrorist financing operations[5] and the proliferation of weapons of mass destruction[6];
- allow compliance with the restrictive measures and the prohibition under Italian Law 220/2021[7].

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, terrorist financing and the proliferation of weapons of mass destruction, and non-compliance with the restrictive

---

[4] 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.

[5] Terrorist financing: any activity, using any means, for the purpose of collecting, financing, brokering, storing, holding in custody or disbursing funds or economic resources, however they are performed, 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 to commit said offences.

[6] Financing of programmes for the proliferation of weapons of mass destruction: the provision or collection of funds and economic resources, carried out in any manner and instrumental, directly or indirectly, to supporting or fostering all those activities related to the design or implementation of programmes aimed at developing nuclear, chemical or bacteriological warfare tools.

[7] Law 220/2021 provides for the total prohibition of the financing of companies in any legal form established, having their registered office in Italy or abroad, which, directly or through subsidiaries or associates, carry out activities involving the construction, production, development, assembly, repair, preservation, utilisation, use, storing, storage, possession, promotion, sale, distribution, import, export, transfer or transport of anti-personnel mines, cluster ammunitions and submunitions, of any nature or composition, or parts thereof.

measures and with the prohibition under Italian Law 220/2021, as well as measures to prevent the risk to which they are exposed;
- the accountability of employees and non-employed staff;
- the clear definition, at the various levels, of roles, tasks and responsibilities as well as the introduction of procedures designed to ensure compliance with the obligations of:

  - customer due diligence[8], reporting of suspicious transactions[9], retention of documentation and evidence of ongoing relationships[10] and transactions[11];
  - compliance withthe restrictive measures and with the prohibition under Italian Law 220/2021;

- the establishment of a special function in charge of supervising the activities of:

  - preventing and managing the risks of money laundering, terrorist financing and the proliferation of weapons of mass destruction;
  - complying with the restrictive measures and with the prohibitions under Italian Law 220/2021;

- a system of Internal Control Functions (hereinafter ICF), 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 non-employed 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, terrorist financing and the proliferation of weapons of mass destruction, as well as non-compliance with

---

[8] 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.

[9] 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.

[10] 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.

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

the restrictive measures and with the prohibition under Italian Law 220/2021, extending them also to those areas not directly envisaged through a full knowledge of the counterparty.

2.1 Risk exposure assessment

The assessment of the Group's exposure to the risk of money-laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as non-compliance with the restrictive measures and with the prohibition under Italian Law 220/2021 is carried out by the Parent Company's Anti-Money Laundering function through an internal self-assessment, which also concerns the individual subsidiaries, therefore providing an integrated assessment of the risk exposure of the entire Group. [12]

The self-assessment exercise is carried out with reference to the individual Group companies, obliged entities pursuant to Italian Legislative Decree 231/2007 or relevant national legislation, including the companies that have not outsourced the anti-laundering function to the Parent Company's Anti-Money Laundering Function, which act independently under the coordination of the Parent Company's Anti-Money Laundering Function.

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 Parent Company or the other Group companies. The 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 received by the corporate bodies as well as of every regulatory, process and safeguard aspect connected to the same. For the purpose of the inherent risk assessment, the Group does not promote business proposals involving cryptocurrencies and, more generally, crypto activities.

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, taking into account the indications provided in the Annual Report prepared by the AML function and approved by the Board of Directors. For the Group companies that have not outsourced the anti-money laundering function to the Parent Company's Anti-Money Laundering Function, the remedial

[12] Hereinafter, the risk of money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as non-compliance with the restrictive measures and with the prohibition under Italian Law 220/2021 is reported as: of the risks to which the Group is actually exposed.

actions are proposed by the Chief Executive Officer of the individual company, approved by its Board of Directors and notified to the Parent Company's Anti-Money Laundering Function.

The Parent Company's Anti-money Laundering Function coordinates and monitors the implementation of the identified remedial actions and verifies, on an ongoing basis, their suitability in order to ensure adequate prevention and mitigation of the risks to which the Group is actually exposed; in addition, in consideration of the annual results of the Group's self-assessment exercise, the Parent Company's Anti-Money Laundering Function defines and implements targeted actions aimed at spreading a corporate culture focused on the prevention of the risks assessed during the exercise.

2.2 Due Diligence and Know Your Customer activities

Due Diligence and Know Your Customer activities are the cornerstone of the prevention of the risks to which the Group is actually exposed 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, as 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, whenever any doubts arise as to the correctness of the information already acquired and if elements arousing suspicion of money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as violation of the restrictive measures or the prohibition under Italian Law 220/2021, are encountered, regardless of any derogation, exemption or threshold that may apply.

In compliance with the risk-based approach, the monitoring model adopted by each Group entity carrying out financial activities provides for a due diligence process tailored to the specific level of risk, also taking into account the nature and purpose of the account or occasional transaction, and also making use of specific authorisation processes to allow the establishment or continuation of ongoing relationships in the case of customers classified as high risk.

The mere fact that they belong to commercial categories deemed to have a potential greater risk of money laundering can never result in the application of a generalised de-risking[13]. Any refusal or interruption of relationships, to be considered for each individual customer, must be assessed in a timely manner and, based on the adopted risk management approach, hinges on an objective analysis and the application of measures of enhanced due diligence, as indicated in this Regulation.

In any event, in addition to the conduct of the customer and the nature of the transaction or account, the following are deemed to be important: the risk elements linked to the specific

[13] By generalised de-risking, we are here referring to the refusal or interruption of relationships with individual customers or entire categories of customers simply because they are considered to be at high risk of money laundering or terrorist financing.

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 with reference to the suitability of the prevention systems adopted in terms of management of the risk of money laundering, terrorist financing and the proliferation of weapons of mass destruction or the exposure to restrictive 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, the executing parties and the beneficiaries (if any), their 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 their 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, and the beneficiaries (if any), but also the beneficial owner must always be identified, according to primary provisions and the detailed indications reported 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, inter alia, the riskiness of the economic sector in which the customers operate.

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 reliable and independent sources, including through the use of automated control procedures integrated with public sources. In particular, the fulfilment of due diligence obligations includes verifying whether the persons identified belong to watchlists for combating money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as non-compliance with the restrictive measures and with the prohibition under Italian Law 220/2021. 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 risks to which the Group is actually exposed.

These activities, together with monitoring activities, make it possible to continuously oversee the risks to which the Group is actually exposed, thus continuously contributing to defining the overall risk level represented within the Group's self-assessment exercise.

Similar measures are also taken with regard to counterparties, even though these are not the direct recipients of the due diligence 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 set of information 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 due diligence obligations are considered to have been met through an appropriate certification issued by the third party that has fulfilled them directly in relation to the establishment of an ongoing relationship or the execution of an occasional transaction.

Group companies may delegate the fulfilment of customer due diligence obligations to a third party by virtue of a specific distribution agreement. The distribution agreements must include the procedures for issuing the certification and must provide that, on request, the third parties are able to promptly submit a copy of the documents and information collected.

The Group parties carrying out financial activities are responsible for the due diligence and assess whether the information collected and the checks conducted out by the third parties are up-to-date, suitable and sufficient for fulfilling the obligations. Where this is not the case, they shall directly fulfill the due diligence obligations and, where this is not possible, refrain from establishing the ongoing relationship or executing the transaction, assessing whether to report a suspicious transaction.

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 money laundering activities resulting from or connected to 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 Parent Company's AML function.

Alternatively, without prejudice to the acquisition of a copy of a valid identity document, a customer can be identified remotely according to a registration procedure based on

technological solutions provided by external operators and recognised by the market or through the use of national or European public digital identification/portfolio systems.

Alternatively, in the event of remote identification, a copy of a valid identity document must be obtained, a transfer must be made from a bank account in the same name or joint names 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 or suspicions.

The remote identification solutions are subject to prior assessment by the Parent Company's Anti-Money Laundering Function to verify their compliance, including as regards their suitability to detect money laundering, terrorist financing and the proliferation of weapons of mass destruction, and to periodically review the rules adopted by all the relevant Functions.

If irregularities or suspicions 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.

2.2.4 Simplified due diligence

If the risk to which the Group is actually exposed is low, due diligence requirements are simplified by reducing the scope and frequency of the related obligations. The model adopted envisages a due diligence process, which provides a set of information that differs from that 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 to which the Group is actually exposed is high, due diligence requirements are simplified by expanding the scope, depth and frequency of the related obligations.

The model adopted envisages a due diligence process, which provides a set of information that differs from that collected in the ordinary due diligence process. Specifically, enhanced due diligence measures are carried out through the acquisition of more information on the customer, the beneficial owner and, if present, the beneficiaries, as well as a more accurate assessment of the nature and purpose of the relationship.

Intensification of the frequency of checks and greater scope and 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 to cases in which a higher risk of money laundering is found as governed by the operating regulations and, in any case, in the event of:

a) opening of an ongoing relationship or execution of transactions with customers and their beneficial owners who hold the status of politically exposed person (PEP);

b) opening of an ongoing relationship or execution of transactions with customers and associated beneficial owners resident or domiciled in third countries with a high risk of money laundering[14];

c) opening of a cross-border correspondent account with a credit institution or corresponding financial institution in a third country.

The enhanced due diligence measures referred to above are operationally scaled based on the proportionality principle[15].

In the above three cases, authorisation by a senior manager[16]is required.

In support of the decision to be taken, a preliminary investigation is carried out which involves a greater in-depth analysis of the information related to the customer and to any parties connected by family or business ties, the beneficial owners and to the purpose and nature of the account or transaction, the origin of the funds used or their destination and the relationship between the parties involved, in order to be able to assess the soundness of the controls put in place to prevent the risk of money laundering and terrorist financing, as well as the potential exposure in terms of reputational risk.

The set of documents to be acquired also depends on the headquarters of the customer, the parent company or the beneficial owner.

In the event of a request to set up or continue an ongoing relationship in the three cases indicated above, Anti-Money Laundering provides its opinion prior to the decision of the senior executive.

The opinion is expressed according to a methodology based on proportionality principles and a risk-based approach, in order to focus the specialist assessment on the most significant and relevant events to improve the effectiveness of the management and prevention of money-laundering risk.

In this regard, with reference to politically exposed persons, Anti-Money Laundering continuously checks the personal data of each new or existing customer using lists of external providers and, if a match is found, conducts a prompt check to detect any prejudicial elements[17].

---

[14] High-risk countries are those identified on a case-by-case basis by the European Commission (contained in EU Regulation 2016/1675) in addition to those identified by the Ministry of Economy and Finance.

[15] Also by setting materiality thresholds, the assessment of the risk profile attributed to the customer and the reasons for setting up the account or the execution of the transaction.

[16] 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 related to this level of risk. In the case of subsidiaries, the authorisation power is held by the party holding powers of administration or management, with the right to delegate in favour of a member of their staff or to another party exercising equivalent functions.

[17] Reports of suspicious transactions carried out in the last three years, requests for assessment by the judicial authorities, seizure or confiscation orders, inclusion in the lists of providers that identify parties subject to national

For politically exposed persons, as well as for customers and associated beneficial owners resident or domiciled in third countries at a high risk of money laundering, the absence of prejudicial evidence will generate an immediate authorisation to proceed from Anti-Money Laundering.

The presence of prejudicial evidence detected automatically, or of any significant elements detected by the commercial network as part of the preliminary investigation procedure, on the other hand, entails the issue of an opinion by Anti-Money Laundering regarding the evidence brought to light and the possibility that it may prejudice the initiation or continuation of the relationship.

If the senior executive decides not to comply with the Anti-Money Laundering opinion, he/she is required to formalise and justify the decision and to identify the measures to be adopted to mitigate the risks reported.

For politically exposed persons, the status is extended for up to one year from the cessation of public office.

With reference to continuous relationships and transactions involving high-risk third countries, it is in any case compulsory to refrain from establishing or continuing relationships or carrying out transactions that directly or indirectly involve trust companies, trusts, limited companies (or those controlled through bearer shares) or shell banks based in high-risk third countries.

Second-level controls on cryptocurrency transactions and more generally crypto activities 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[18] and the customer's relationships with related parties, the provisions of which are specified and periodically reviewed by the AML function.

For the Group companies that use the same profiling model, the harmonisation of the risk profile assigned to the customer prudentially guarantees the application of the safeguards

---

or local press reports relating to offences of a criminal nature or ongoing investigations must always be taken into consideration.

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

provided for by the highest risk band.[19] The obligation remains for all Group companies to adopt a profiling model that is homogeneous and consistent with that adopted by the Parent Company.

In this sense, in compliance with the risk-based approach, the financial intermediaries belonging to the Group, also taking into account specific business and customers characteristics, determine their risk bands at no less than four.

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. In all cases where, at the time of updating the risk profile, the continuation of an ongoing relationship is subject by law to authorisation by a senior manager, the opinion of the Anti-Money Laundering function must be obtained as desribed in the paragraph “Enhanced due diligence".

For customers included in the highest risk band, the risk profile must be updated with a frequency of no more than 12 months. For the other bands, the minimum update frequency can be differentiated. Renewal may be carried out through automated tools only in lower-risk cases and, in any case, where there are no elements requiring specific assessment.

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, which must document in writing the reasons for such decision.

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

The model adopted envisages specific control measures and rules for the management and monitoring of operations which, due to their objective characteristics, present a higher risk to which the Group is actually exposed, taking into account the results of the self-assessment exercise, the National Risk Assessment and the results of the analysis carried out by the Financial Security Committee[20] on the risk of non-application and evasion of the targeted financial sanctions related to the financing of the proliferation of weapons of mass destruction, as well as the areas of attention highlighted by the Supervisory Authority.

[19] Every month, for all common customers of Banco BPM, Banca Aletti, Banca Akros, Aletti Fiduciaria and Banco BPM Invest SGR, the procedure verifies the risk classification assigned by the aforementioned Group companies, aligning it with the highest risk band.

[20] The Financial Security Committee (FSC), established at the Ministry of Economy and Finance (MEF), monitors the operation of the system for preventing and combating terrorist financing (Italian Law 431/2001) and money laundering (Italian Legislative Decree 231/2007), the activities of countries that threaten international peace and security, the financing of the proliferation of weapons of mass destruction, and implements the freezing measures ordered by the United Nations, the European Union. and at national level (Italian Legislative Decree 109/2007).

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.

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.

The Banco BPM Group also prohibits the opening, in any form, of current accounts and savings passbooks or any other kind of relationship anonymously or in fictitious names.

2.5 Data storage and recording

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 stored 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 stored for the same period.

The model adopted is based on compliance with the applicable data protection provisions and ensures the storage of information, in special archives, relating to transactions, including those involving amounts below the threshold for recording 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 the adopted model and regulatory developments in anti-money laundering, the combating of terrorist financing and the proliferation of weapons of mass destrunction, as well as in the area of restrictive measures, 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 training 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 training ensures that personnel that comes into more direct contact with customers or is in any case involved in the process of reporting suspicious transactions, as well as those assigned to the anti-money laundering function receive specific instruction on these matters.

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 training activities covers not only the contents but also the 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 teaching 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

The Banco BPM Group's organisational model for the prevention and mitigation of the risks to which the Group is actually exposed provides for the involvement of the following:

- 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 Anti-Money Laundering function;
- the Anti-Money Laundering function;
- the Manager in charge of suspicious transaction reporting (known as "STR Delegate");
- the Group Sanction compliance manager;
- the internal audit function;
- the contact or support structures for relations with customers and counterparties.

The Banco BPM Group has adopted a partially centralised model, whereby the subsidiaries subject to the reference regulations can outsource the anti-money laundering function to the Parent Bank's Anti-Money Laundering function and therefore identify specific Anti-Money Laundering contact persons.

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

3.1 Parent Company

Strategic guidelines on management of the risks to which the Group is actually exposed are adopted by the Parent Company's corporate bodies.

The Parent Company ensures that the corporate bodies of the other Group companies implement, within their own organisations, the Group's strategies and policies on the prevention of money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as those on compliance with the restrictive measures and with the prohibition under Italian Law 220/2021, and ensures that the corporate bodies and internal structures of each Group member have the necessary information to be able to carry out the related tasks.

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 to which the Group is actually exposed, for the purpose of ensuring, in line with the risk-

based approach, suitability with respect to the scale and type of risks to which the Banco BPM Group's activities are effectively exposed, as described in the internal risk assessment document;

- approves these Regulations which describe 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, in line with the criteria 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 the risks to which the Group is actually exposed, and ensures its effectiveness over time;
- approves the criteria for handling relations with customers classified as 'high-risk';
- appoints the Officer responsible for anti-money laundering, ensuring that he or she meets the conditions set forth in the reference legislation and ensures that they are promptly informed of any decisions that may affect the exposure to money laundering risk;
- appoints, after consulting the Board of Statutory Auditors, the Head of Anti-Money Laundering, as proposed by the Internal Control and Risks Committee, supported by the Appointments Committee, and revokes the same, after consulting the Board of Statutory Auditors, after hearing the opinion of the Internal Control and Risks Committee, supported by the Appointments Committee;
- appoints and removes the Sanction compliance manager;
- ensures, on an ongoing basis, that the roles and responsibilities for the prevention of money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as those connected to compliance with restrictive measures and with the prohibition under Italian Law No. 220/2021, are clearly specified and appropriately assigned, guaranteeing that operational and control functions are separated and that these functions are given resources that are adequate in qualitative and quantitative terms;
- ensures that an adequate, complete and timely system of information flows is in place towards the corporate bodies ("vertical flows") and between control functions ("horizontal flows"); In order to guarantee and facilitate coordination between the control functions and the corporate bodies, a shared methodology for assessing the Group's internal control system is adopted and integrated operating methods are established to ensure the exchange of information;
- ensures confidentiality is maintained within the suspicious transaction reporting procedure;
- at least annually, examines the report on the activities of the Anti-Money Laundering Function at group level, as well as the document on the results of the self-assessment of the risks to which the Group is actually exposed, which must also include the activities and risks of potential non-application or evasion of financial sanctions, including those related to the financing of the proliferation of weapons of mass destruction. With the same frequency, it assesses the activities of the Anti-Money Laundering function and the

adequacy of the human and technical resources assigned to it, also in light of the periodic verification carried out by the internal audit function;

- 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 risks to which the Group is actually exposed, identifying the safeguards to mitigate them, the effectiveness of which it assesses.

3.1.2 Board of Statutory Auditors

The Board of Statutory Auditors, as a body charged with control, monitors compliance with regulations and the completeness, functionality and adequacy of the control systems with regard to anti-money laundering, combating terrorist financing, preventing terrorist financing activities, and the proliferation of weapons of mass destruction, as well as the activities related to compliance with the restrictive measures and the prohibition under Italian Law 220/2021. 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's Head of Anti-Money Laundering 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, terrorist financing and the proliferation of weapons of mass destruction, as well as non-compliance with the restrictive measures and the prohibition under Italian Law 220/2021.

The members of the Board of Statutory Auditors shall promptly inform the Supervisory Authority 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.

3.1.3 Supervisory Body pursuant to Italian Legislative Decree 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.

3.1.4 Representative responsible for anti-money laundering

The Board of Directors, at the time of its renewal, assigns to one of its members, in accordance with the indications of the Supervisory Authority, the role of Representative responsible for anti-money laundering of the Parent Company.

The latter, specifically:

- constitutes the main point of contact between the Head of Anti-Money Laundering and the Board of Directors and ensures that the latter has the information required to fully understand the relevance of money laundering risks;
- monitors that the policies are adequate and proportionate, taking into account the characteristics of the recipient and the risks to which it is exposed;
- assists the Board of Directors in assessments concerning the organisational structure and the allocation of Anti-Money Laundering resources;
- ensures that the corporate bodies are periodically informed about the activities carried out by the Anti-Money Laundering Manager, and on any discussions with the Authorities, guaranteeing information flows in line with what is defined by the Integrated Internal Control System Regulation (RE 313);
- informs the corporate bodies of the violations and critical issues concerning anti-money laundering of which it has become aware and recommends the appropriate actions;
- verifies that the Head of Anti-Money Laundering and the Sanction compliance manager have direct access to all the information they need in order to fulfil their duties;
- verifies that the Head of Anti-Money Laundering has direct access to all the information necessary for the performance of his/her duties, that he/she has sufficient human and technical resources and tools, that he/she is informed of any deficiencies relating to anti-money laundering identified by the other internal control functions or by the Supervisory Authorities and that the problems and proposals for action proposed by the same are appropriately assessed.

The Representative responsible for anti-money laundering of the Parent Company is the same as the Representative responsible for anti-money laundering at the Group level.

The individual Group entities assess whether there is a conflict of interest for the party designated as the Representative responsible for anti-money laundering as part of the internal rules governing the requirements and criteria of suitability for the performance of the assignment and management operations and activities in compliance with the organisational and procedural controls in place.

3.1.5 Chief Executive Officer

As the body responsible for performing management functions, the Chief Executive Officer, through the relevant functions:

- oversees the implementation of the strategic guidelines and the policies for managing the risks to which the Group is actually exposed 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 for monitoring the risks to which the Group is actually exposed; to this end, he/she assesses the organisational and procedural actions suggested by the Head of Anti-Money Laundering and formalises any decision not to accept them, thereby providing justification. In setting up operational procedures, takes into account the indications and guidelines issued by the competent authorities and the various international organisations;
- specifies and oversees the implementation of a system of internal controls for the prompt detection and management of the risks to which the Group is actually exposed and ensures its effectiveness over time, according to the results of the internal risk assessment;
- proposes to the Board of Directors and implements, through the Anti-Money Laundering Function, the remedial actions arising from the self-assessment exercise, taking into account the indications set out in the anti-money laundering function's annual report;
- 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 Parent Company and Group companies, 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 oversees 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 the prevention of money laundering, terrorist financing activities and the proliferation of weapons of mass destruction, as well as compliance with the restriction measures and prohibitions under Italian Law 220/2021;
- defines these Regulations, submits them for approval of the Board of Directors and oversees their enforcement;
- specifies and oversees the implementation of information procedures aimed at ensuring that all the corporate units involved and the bodies 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 staff training and education programmes regarding the obligations arising from regulations on the prevention of money laundering, terrorist financing and the proliferation of weapons of mass destruction, as well as compliance with the restriction measures and prohibitions under Italian Law 220/2021, ensuring the continuity and systematic nature of training activities, taking account of developments in the reference regulations and the procedures specified and adopted by the Parent Company and Group companies;
- decides on the instruments to be used to verify the activity carried out by employees and non-employed 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 non-employed 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, terrorist financing and the proliferation of weapons of mass destruction, as well as compliance with the restriction measures and prohibitions under Italian Law 220/2021, with particular reference to the automatic detection of anomalous transactions.

3.1.5 Group Head of Anti-Money Laundering

The Group Head of Anti-Money Laundering must comply with suitable independence, authority, professionalism and reputation requirements. The requirements are assessed in line with the provisions of the Requirement Regulations and suitability criteria for fulfilment of the engagement of company representative for the Banco BPM Group (RE 373).

He/she is included among the heads of CCUs and has no direct responsibility over operational areas subject to control; he/she must not have direct responsibilities over operating areas subject to control, nor report to the persons in charge of said areas;

The Group Head of Anti-Money Laundering reports directly or via the Representative responsible for Anti-Money Laundering, without restriction or intermediation, to the corporate bodies of the Bank and its subsidiaries, including the 231/01 Supervisory Bodies, where set up.

The Group Head of Anti-Money Laundering cooperates with the heads of the Anti-Money Laundering functions of the financial intermediaries belonging to the Group that have not outsourced such a function, including those abroad, and ensures that they carry out their duties in a coordinated fashion and according to the Group's policies and procedures. Specifically:

- coordinates, through the definition of a common methodology, the self-assessment exercise carried out by the financial intermediaries belonging to the Group, giving instructions on the timing and methods for contributing to the exercise, and defining the activity plan, the structure of the information to be provided and the related methods of transmission;
- prepares a Group-wide assessment of the risks to which the Group is actually exposed, taking into account the risks resulting from individual exercises, the interrelations among

the individual Group companies and their impact on risk exposure at group level, and oversees the identification and implementation of remedial actions, continuously verifying the suitability of the measures adopted to ensure adequate control of the risks to which the Group is actually exposed;

- presents to the corporate bodies of the Parent Company an annual report on the exposure to money laundering risks and on the Anti-Money Laundering activities at Group level;
- draws up and submits to the corporate bodies of the Parent Company a series of Group procedures, methodologies and standards on anti-money laundering, the combating of terrorist financing and the proliferation of weapons of mass destruction, and on ensuring compliance with the restrictive measures and the prohibitions under Italian Law 220/2021, and ensures that the policies and procedures of the members of the group are in line with these standards and comply with relevant legislative and regulatory provisions;
- establishes periodic information flows by all Group companies to share the information necessary for the performance of their duties.

3.1.5 Sanction compliance manager

The Sanction compliance manager must comply with suitable independence, authority, professionalism and reputation requirements.

In line with the model for monitoring the risk of failing to implement the restrictive measures, the Parent Company appoints the Head of Anti-Money Laundering of the Parent Company as the individual responsible for assessing the application of the restrictive measures. In the event that the Sanction Compliance Manager is absent or unavailable, he/she is replaced by the Head of Anti-Money Laundering of the Parent Company or by other delegates identified within the same unit.

The Group Sanction compliance amanger has no direct responsibility over operational areas subject to control, nor is hierarchically subordinate to the heads of those areas.

The Group Sanction Compliance Manager reports directly or via the Representative responsible for Anti-Money Laundering, without restriction or intermediation, to the corporate bodies of the Parent Company and its subsidiaries, including the 231/01 Supervisory Bodies, where set up.

Without prejudice to the fact that each financial intermediary belonging to the Group is ultimately responsible for compliance with the restrictive measures, the Sanction compliance manager is tasked with:

- developing, implementing and keeping up to date adequate policies, procedures and controls to ensure compliance by the Group with restrictive measures and proportionate to its exposure to EU and national restrictive measures, assessing the extent to which the Group's activities are exposed to these restrictive measures and vulnerable to being circumvented;
- periodically providing adequate information to both the Board of Directors and the Chief Executive Officer of the Parent Company to allow them to perform their respective functions;

- reporting all violations of restrictive measures to the national authorities competent for the implementation of restrictive measures and/or to the competent supervisory authority in compliance with applicable regulations;
- cooperating effectively and constructively with the national authorities competent for the implementation of restrictive measures and with the competent supervisory authority in compliance with applicable regulations;
- supervising the preparation and delivery of the training programme.

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 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 model for monitoring the risks to which the Group is actually exposed, the Parent Company:

- names the Head of the Anti-Money Laundering function of the Parent Company as the first delegate in charge of assessing the suspicious transaction reports arriving 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 financial intermediaries belonging to the Group 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 their absence or impediment, within the Anti-Money Laundering structure of the Parent Company.

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

- promptly assessing, in the light of all the available information, the suspicious transactions reported by the head of the structure which actually manages relations with customers (so called "first level") and those of which he/she has otherwise become aware during 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.
- forwarding to the FIU the reports that are considered to be appropriately grounded, 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 various capacities in managing and combating money laundering,

terrorist financing and the proliferation of weapons of mass destruction, as well as the application and evasion of restrictive measures. 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 indicated in the suspicious transaction report to be made available - also using suitable IT databases - by the managers of the different operational structures of the Group, given the importance that such information may have when entering into new contractual relationships or assessing transactions of customers already acquired and the counterparties.

The intermediaries or other financial intermediaries belonging to the Group that have not granted a mandate shall send the delegate a copy of the reports sent to the FIU, or closed, including the reason for such a 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 investigating anomalous transactions and relationships from a Group perspective, the delegate may make use of any structure of the subsidiaries, including those that have not granted the proxy; in this regard, he/she shares the relevant information on common customers with the managers of suspicious transaction reports of the financial intermediaries belonging to the Group that have not granted a proxy.

3.2 Other Group companies

The corporate bodies of the financial intermediaries belonging to the Group 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 corporate entities, of the strategies and policies specified on the subject of preventing the risks of involvement in money laundering, international terrorist financing and the proliferation of weapons of mass destruction, as well as non-compliance with the restrictive measures and with the prohibition under Italian Law 220/2021.

The Board of Directors of the financial intermediaries belonging to the Group that fall within the scope of application of Italian Legislative Decree 231/2007, at the time of its renewal, assigns to one of its members or to the General Manager, in accordance with the indications of the Supervisory Authority, the role of Representative responsible for anti-money laundering. The responsibilities are those described in the Regulation with reference to the Parent Company, to be carried out in line with the management and coordination activities of the Representative responsible for anti-money laundering at the Group level.

3.2.1 Financial intermediaries belonging to the Group that have outsourced the anti-money laundering function to the Parent Company

With regard to the centralised model, through which the 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 the same requirements of independence, competence, professionalism and reputation as those envisaged for the Group Head of Anti-Money Laundering;
- have direct access, together with the Group Head of Anti-Money Laundering, to the corporate bodies of the Bank or company 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;
- ensure on an ongoing basis that the management body is adequately informed about the performance of the outsourced activities;
- they constantly monitor the timely and correct performance of the outsourced activities, in relation to which they promptly, independently and directly inform the company bodies of any violations of the obligations set out in the outsourcing contract;
- collaborate in drawing up plans for all control activities within their remit, as set out in the Annual Reports, to be submitted to the Board of Directors of the Parent Company and of the Bank or Company.

3.2.2 Financial intermediaries belonging to the Group that have not outsourced the anti-money laundering function to the Parent Company

The roles and responsibilities of the Anti-money Laundering Function of the financial intermediaries belonging to the Group, where not centralised, are those defined by these Regulations, the supervisory provisions that apply to the sector, local regulations for foreign subsidiaries, and the specific operating nature of each single company.

The foreign subsidiaries establish, as part of the regulatory compliance function, a structure for the prevention of the risk of money laundering, terrorist financing and the proliferation of weapons of mass destruction, if not already provided for by local regulations in force. The Head of Regulatory Compliance, together with General Management, is tasked with handling the information flows to local Supervisory Authorities. The foreign subsidiaries carry out the activities in compliance with the regulations of their own country and define, with the Anti-Money Laundering function of the controlling company and, if applicable, with the Anti-Money Laundering of the Parent Company, the information flows necessary for the risk assessment, in order to ensure their adequate valuation within the Group's annual self-assessment.

The relationship between the Anti-Money Laundering function of the Parent Company, which is responsible for guidance, coordination and control, and the corresponding functions within the financial intermediaries belonging to the Group that have not outsourced them to the Parent Company, is carried out according to the principles defined by the 'Banco BPM Group Governance Regulation' (RE 303) on functional dependence.

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 regarding the prevention of money laundering, terrorist financing and the proliferation of weapons of mass destruction, and the application of the restrictive measures and the prohibition under Italian Law 220/2021.

Pursuant to the supervisory provisions, the AML function is guaranteed the necessary independence. The AML function is given adequate economic resources, the 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 terms of number, technical and professional skills and their professional development must be ensured, including 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 Head of the Group Anti-Money Laundering function, are responsible for:

- cooperating in defining the policies for managing the risks to which the Group is actually exposed and the various stages of the risk management processes;
- cooperating in defining the system of internal controls and procedures aimed at preventing and combating the risks to which the Group is actually exposed, and identifying the factors to be taken into account in assessing the risk of the parties assessed;
- providing support and assistance to corporate bodies;
- identifying the applicable provisions and, with reference to these, verifying on an ongoing basis the adequacy of the process for managing the risks to which the Group is actually exposed and the suitability of the system of internal controls and procedures, and proposing organisational and procedural changes aimed at ensuring adequate supervision of these 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;
- continuously verifying the effectiveness of policies and procedures for the remote identification of customers;
- issuing a prior opinion to initiate or continue a relationship in cases where the authorisation of a senior manager is required (by law) in accordance with the provisions of the Regulation;

- in liaison with the manager in charge of suspicious transaction reporting, conducting checks on the functionality of the reporting process and on the appropriateness of the assessments made by the first level on customer operations;
- defining procedures for the management of suspicious transaction reports (originating from the so-called first level) regarding particularly high risk situations to be treated with due urgency;
- conducting, in liaison with the other corporate functions concerned, the annual internal assessment on the risks to which the Group is actually exposed;
- preventively assessing the risks to which the Group is actually exposed related to the offer of new products and services, the significant modification of products or services already on offer, the entry into a new market or the start of new activities and recommending the necessary measures to mitigate and manage these risks, as governed by the Regulation on the approval of new products and markets and product distribution (RE 338);
- verifying the reliability of the information system for the fulfilment of the obligations of customer due diligence, data retention and suspicious transaction reporting;
- sending to the Supervisory Authority responsible for the specific area, within the set deadlines, objective communications concerning transactions at risk of money laundering, the aggregate data concerning the overall operations and periodic anti-money laundering reports;
- in liaison with the other corporate units responsible for training, preparing an adequate training plan aimed at ensuring continuous personnel development and updating, overseeing the structuring of effectiveness indicators for the training activities performed and taking part, through direct involvement of its own resources, in the teaching activities;
- preparing the periodic information flows to the corporate bodies and to the Representative responsible for anti-money laundering, in accordance with the provisions of the Integrated Internal Control System Regulation (RE 313);
- 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;
- promptly informing the corporate bodies of violations or significant shortcomings found in the exercise of their duties;
- informing the corporate bodies on a regular basis on the progress of the corrective actions adopted in the event of deficiencies found in the control activity and the possible inadequacy of the human and technical resources assigned to the anti-money laundering function and the need to reinforce them;
- 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, terrorist financing, the proliferation of weapons of mass destruction or the evasion of the restrictive measures, 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 non-employed 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.

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

The internal audit function regularly verifies the risk self-assessment exercise conducted by the Anti-Money Laundering Function.

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.