GUIDELINES FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING AND FOR MANAGING EMBARGOES

Rules applicable to sensitive areas relating to Legislative Decree 231/01
Risk area: Offences against the public administration
Protocols: Management of relations with Supervisory Authorities
Risk area: Crimes related to terrorism or against democracy, organised crime, international crime and crimes against the individual
Risk area: Handling stolen goods, money laundering, handling of illegally gained assets or cash and self-laundering
Protocols: Combating terrorist financing and laundering of the proceeds of crime
Risk area: Computer crime
Protocols: Management and use of computer systems and the Group's Company Records

Document Owner:
Anti Financial Crime Head Office Department

Recipients:
Intesa Sanpaolo Group

Path:
ARCO – Foreign Network – Headquarter Governance Documents – Governance Documents – Guidelines

Effective from: December 2019

INTESA SANPAOLO

CONTENTS

1. INTRODUCTION

The Intesa Sanpaolo Group acknowledges the strategic significance of monitoring compliance risk and conduct risk, included in the governance system for combating money laundering and terrorist financing and for managing embargoes.

The Guidelines in this document, which have been written also in compliance with the Bank of Italy's Regulations of 26 March and 30 July 2019[1], identify the applicable standards and define the risk management model regarding money laundering, terrorist financing and breach of embargoes of Intesa Sanpaolo, setting out:

- the general principles of the governance model;
- the roles and responsibilities;
- the macro-processes for combating money laundering and terrorist financing and for managing embargoes;
- Group governance.

The Guidelines are reviewed on an annual basis and any amendments are subject to the approval of the Board of Directors, after review by the Risks Committee and Management Control Committee.

The Guidelines are set out in operational terms in the Rules for Managing Compliance Macro-Processes (Compliance Rulebook) and in the Company Rules on anti-money laundering, combating terrorist financing and managing embargoes, which define specific, individual obligations. The Compliance Rulebook is reviewed annually, in keeping with organisational and operational changes to the risk management model for money laundering, terrorist financing and the breach of embargoes, and any changes are approved by the Chief Compliance Officer and put to the attention of the Management Control Committee. The Compliance Rulebook is issued with an Internal Note of the Chief Compliance Officer.

"Money laundering" means:

- the conversion or transfer of assets, carried out in the knowledge that they originate from criminal activity or from participation in such activity, for the purpose of concealing or disguising the unlawful origin of the assets or assisting anyone involved in this activity to avoid the legal consequences of their actions. Money laundering also means the use and hiding of the proceeds of unlawful origin by persons who committed the offence generating the proceeds ("self-laundering");
- concealing or disguising of the true nature, origin, location, availability, movement, ownership of the assets or the rights thereto, carried out in the knowledge that they originate from criminal activity or from participation in such activity;
- purchase, holding or use of assets, in the knowledge, at the time of their receipt, that said assets originate from criminal activity or from participation in such activity;
- participation in one of the actions referred to in the above points, association for the purpose of committing said action, attempt to perpetrate it, assisting, instigating or advising someone to commit it or facilitating its execution.

“Terrorist financing" means any activity directed, using any means, at providing, collecting, funding, brokering, depositing, keeping safe or disbursing, in any way, funds or economic resources, directly or indirectly, in whole or in part, destined to be used to carry out one or more types of behaviour, for the purpose of terrorism in accordance with criminal laws, regardless of whether the funds or economic resources are actually used for committing said actions.

[1] These regulations require, inter alia, the approval by the supervisory body of a specific "anti-money laundering policy".

“Embargo” means the ban on trade and exchange with Countries subject to sanctions, in order to isolate and put their governments in a difficult position with regard to their domestic policy and economy.

2. LEGAL FRAMEWORK

2.1 The legal framework for anti-money laundering and combating terrorist financing

The main legislation on preventing and combating money laundering and terrorist financing may be classified as follows:

- EU legal instruments;
- primary and secondary Italian legislation.

Main European Union law is as follows:

- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 (the "IV Directive") on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30/05/2018 ("V Directive"), amending Directive EU 2015/849;
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;
- Commission Delegated Regulation (EU) 2016/1675, as amended, supplementing the IV Directive by identifying high-risk third Countries with strategic deficiencies;
- Commission Delegated Regulation (EU) 2019/758 supplementing the IV Directive with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third Countries (outside the European Economic Area, the "non-EEA Countries");

and, specifically, on money laundering and terrorist financing:

- Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism;
- Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban.

The main primary Italian laws are set out in the following decrees:

- Legislative Decree no. 231/2007, as amended by Legislative Decree no. 125/2019, aligning Italian legislation on anti-money laundering implementing the V Directive;
- Legislative Decree no. 109/2007 as amended by Legislative Decree no. 90/2017, on measures to prevent, combat and repress the financing of international terrorism, establishing obligations to disclose frozen assets and resources and to report suspicious transactions.

The main secondary legislation, issued by the Bank of Italy and the Financial Intelligence Unit (FIU), is contained in the following:

- Regulation of 24 August 2010 on anomaly indicators for intermediaries to facilitate the identification of suspicious transactions;
- Regulation of 3 April 2013 implementing rules for keeping the Single Electronic Archive and for simplified registration procedures[2];
- Regulation of 23 December 2013 for sending aggregate anti-money laundering reporting;

[2] At the time of going to press, the Bank of Italy regulation with specification provisions on the retention and use of data and information for anti-money laundering purposes and for combating terrorist financing, implementing Article 34, paragraph 3 of Legislative Decree no. 231/2007, as last amended by Legislative Decree no. 125/2019, implementing the V Directive, had not yet been issued.

- Regulation of 26 March 2019 on implementing provisions regarding the organisation, procedures and internal controls to prevent the use of intermediaries and other entities performing financial activities for the purposes of money laundering and terrorist financing;
- Regulation of 28 March 2019 on instructions concerning objective notices;
- Regulation of 30 July 2019 on implementing provisions concerning customer due diligence.

The regulations issued by US Authorities, included mainly in the following provisions, are also of particular significance in view of the Intesa Sanpaolo Group operations in the United States:

- Bank Secrecy Act – "BSA" (1970), designed to identify the source, volume and currency of financial instruments that flow into and out of the United States or are deposited with their financial institutions;
- US Patriot Act (Uniting and Strengthening America by Providing Appropriate Tool to Intercept and Obstruct Terrorism - 2001) issued following the terrorist attacks of 11 September 2001, which extends the requirements of the Bank Secrecy Act to banks, requiring them to prepare due diligence procedures and improve information sharing with financial institutions and the US Government;
- Law 302 - Section 504 (NY DFS Rule on Transaction Monitoring and Filtering - 2017) which establishes minimum standards for monitoring transactions and sanctions on Banks subject to New York laws, including the jurisdiction of the New York Department of Financial Service;
- Department of the Treasury Financial Crimes Enforcement Network, ('31 Code of Federal Regulation Parts 1010, 1020, 1023, 1024, and 1026 Customer Due Diligence Requirements for Financial Institutions') that defines the new requirements in terms of identification of the beneficial owner and establishes a control-based approach based on both substantive and formal standards.

As the Intesa Sanpaolo Group operates in the United States it has signed the "US Patriot Act Certification" and is required to observe US law in its business and financial transactions carried out in the United States, such as payment orders in dollars, and in general, in transactions carried out on its own behalf and on behalf of third parties. The transactions that the Bank undertakes on its own account and/or on behalf of its customers are also subject to United States laws when these transactions involve a relationship with parties subject to US legislation (for example US banks, foreign branches of US banks and US Subjects in general).

The common principles of the applicable legal framework are:

- the obligation to carry out customer due diligence, obtaining suitable information to identify the customer, the beneficial owner and the purpose of the account or transaction;
- the obligation to retain data for anti-money laundering obligations;
- the obligation to constantly monitor account transactions;
- the obligation to report suspicious transactions with a view to actively cooperating with the Authorities;
- the obligation not to open a new account, carry out an occasional transaction or maintain an existing account if the due diligence obligations cannot be fulfilled or if there is a suspicion of money laundering or terrorist financing;
- the obligation of the Control Body to report any relevant offences that it becomes aware of when carrying out its duties.
- the obligation for adequate personnel training to ensure the correct application of the provisions.

To meet these obligations, recipients must identify organisational functions, resources and procedures that are consistent with and proportionate to the type of activity carried out, their dimensions, organisational complexity and operating characteristics.

The organisation required by law must be based on:

- the establishment of a specific function to prevent and combat money laundering and terrorist financing transactions, the appointment of a person in charge and of an officer to report suspected money laundering/terrorist financing;

- a clear definition of roles, duties and responsibilities, and procedures that guarantee compliance with customer due diligence and suspicious activity reporting obligations, as well as obligations to store documentation and records of the accounts and transactions and suspicious activity reporting;
- a system of control functions that is coordinated, also through suitable information flows and is adequate for the size of the company and its complexity, and for the type of services and products offered as well as the extent of risk that may be associated with the characteristics of customers;
- a strong emphasis on the accountability of employees and external staff and controls that are suitable for monitoring their compliance with regulatory obligations and internal processes as well as their adoption.

The regulation requires effective coordination of controls for the prevention and combating of money laundering and terrorist financing at a Group level, and the procedures adopted by the Company and Foreign Branches to be in line with Group standards and ensure that information is shared at consolidated level. In the case of non-EEA Countries which have limits on the circulation of information, specific corrective measures shall be adopted, in line with the provisions of the aforementioned Commission Delegated Regulation (EU) 2019/758.

2.2 The legal framework concerning embargoes

The United Nations Charter grants the UN Security Council the power to make binding decisions for all United Nations Member States regarding restrictive measures to encourage the keeping or restoring of international peace and security. The Treaty on European Union and the Treaty on the Functioning of the European Union require Member States to adopt a common position on interrupting or limiting economic and financial relations with one or more non-EEA Countries. The purpose of these measures is to:

- safeguard the values, fundamental interests, security, independence and integrity of the European Union;
- consolidate and support democracy, the rule of law, human rights and the principles of international law;
- preserve peace, prevent conflicts and strengthen international security, in accordance with the purposes and principles of the United Nations Charter;
- promote international cooperation.

There are also other sources deriving from the international context that establish a specific regime prohibiting investment in certain industrial or import/export sectors to and from “high or significant risk" Countries.

Applicable legislation on the management of embargoes may be classified as follows:

- European legal instruments;
- primary and secondary Italian legislation.

Main European law includes:

- Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

Italian primary law includes:

- Law no. 185/1990, as amended on "New rules on the control of exports, imports and transit of weapons”, which remains the fundamental regulation for the transfer of assets classified as weapons;
- Legislative Decree no. 221/2017, which amended and simplified procedures on the authorisation to export dual-use products and technologies and sanctions on commercial embargoes, as well as all types of exports of proliferation materials.

Articles 18 to 21 of the decree provide for criminal and administrative sanctions for anyone who undertakes the export of dual-use goods, in breach of laws.

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

- Regulation of 27 May 2009 containing operating instructions for the exercise of enhanced controls against the financing of weapons of mass destruction proliferation programmes.

As the Intesa Sanpaolo Group operates in the United States, US legislation, comprising the "US Patriot Act" mentioned above, as well as regulations on economic and commercial sanctions adopted by the US Government, mainly through the Office of Foreign Asset Control (OFAC) of the Treasury Department, as part of foreign and national security policies, are of particular importance[3].

The applicable legal framework, which has obvious connections with legislation on money laundering and terrorist financing, mentioned above, establishes restrictive measures and sanctions against governments of third Countries, non-government organisations, and natural or legal persons in relation to:

- arms embargoes;
- other specific or general commercial restrictions (ban on export and import);
- financial restrictions (freezing of assets and resources, bans concerning financial transactions, restrictions on export credits or investments);
- criminal sanctions for entities financing terrorist or subversive associations and exporting dual-use products in breach of regulations governing dual-use.

The legal framework requires the Bank to adopt measures guaranteeing:

- controls of records and customer transactions, regarding imports and/or exports;
- the traceability of controls on transactions originating from/for Countries, persons and entities against whom restrictions have been established;
- the freezing of goods and resources attributable to designated parties that the restrictive measures apply to, and forwarding the resulting communications to the Financial Intelligence Unit (FIU);
- the reporting of transactions suspected to finance terrorism or activities for the proliferation of weapons of mass destruction.

[3] At the time of going to press, this legislation mainly referred to regulations against Iran, Syria, North Korea, Cuba, Venezuela and the Crimea region.

3. GENERAL PRINCIPLES OF THE GOVERNANCE MODEL

These Guidelines fall within the scope of the structure defined by the Group through the Integrated Internal Control System Regulation ("IICS Regulation").

The risk monitoring on money laundering, terrorist financing and breach of embargoes forms an integral part of that system and is pursued through the joint operation of all the company components, in accordance with the provisions of Bank of Italy Regulation of 26 March 2019 in terms of organisation, procedures and internal controls. Specifically:

- in accordance with their duties and responsibilities, the Corporate Bodies will ensure adequate control over the risks of money laundering, terrorist financing and breach of embargoes;
- the Supervisory Board, in accordance with Legislative Decree no. 231/2001, monitors the efficient implementation, function, compliance and update of the relative Model and its ability to prevent and combat the commission of the crimes described in this Decree;
- the Anti-Money Laundering Function continuously checks corporate processes and procedures, and proposes, in association with the applicable corporate functions, the organisational and procedural changes required and/or advisable to ensure adequate control over the risk of money laundering, terrorist financing and breach of embargoes;
- other second level Corporate Control Functions and the support Functions work with the Anti-Money Laundering Function so that it can develop its own risk management procedures that are consistent with corporate strategies and operations;
- the operational, business and support functions follow the corporate processes and procedures, verifying their implementation through appropriate level I controls, with a view to full and complete compliance with applicable laws and standards of conduct;
- The Head of the Internal Auditing Function, within the scope of his/her ordinary activities, monitors the degree of adequacy of the corporate organisational structure and its compliance with applicable laws on an ongoing basis, and also oversees the functioning of the entire internal control system.

In monitoring risks relating to money laundering, terrorist financing and breach of embargoes, the Intesa Sanpaolo Group has adopted the following general standards:

- being inspired by values of honesty, integrity and responsibility; in compliance with the Group's Code of Ethics;
- active cooperation with the Supervisory Authorities to prevent the issues in question, taking into account regulatory provisions on the confidentiality of reporting and information concerning suspicious transactions, the protection of personal data (privacy) and “banking secrecy”;
- the adoption of monitoring standards in terms of guidelines, rules, methods, processes and instruments that are aligned with applicable international standards and are reasonably uniform at a Group level, in compliance with applicable regulations at a local level;
- the adoption of ‘risk-based’ control measures that are proportionate to the characteristics and complexity of the activity carried out, and to the legal status, size and organisational structure of various Group entities.

4. ROLES AND RESPONSIBILITIES

4.1 Corporate Bodies

In accordance with their duties and responsibilities, the Corporate Bodies of the Parent Company are responsible for ensuring the adequate control of the risks of money laundering, terrorist financing or the breach of embargoes to which the Group is or could be exposed. The duties and responsibilities assigned to Corporate Bodies of the Parent Company are set out in relative Regulations and, with reference to the internal control system, in the "IICS Regulation".

4.2 Surveillance Body pursuant to Legislative Decree no. 231/2001

The duties and powers of the Surveillance Body are described in the Organisation, management and control model pursuant to Legislative Decree no. 231/2001. The Surveillance Body, in particular, is in charge of continuously monitoring the efficient implementation, function, compliance and update of the Model and its ability to prevent and combat the commission of the crimes described in the Decree.

4.3 Chief Compliance Officer Governance Area

The duties and responsibilities of the Chief Compliance Officer Governance Area and entities directly reporting to it are described in the Organizational Code of the structures, in the "IICS Regulation" and in the Group's Compliance Guidelines.

The Chief Compliance Officer ensures oversight of the risks of money laundering, terrorist financing and breach of embargoes, through the Anti Financial Crime Head Office Department, which holds the role of “Anti-Money Laundering Function of the Parent Company” and through the Compliance Governance and Controls Head Office Department.

4.3.1 Anti Financial Crime Head Office Department

The duties and responsibilities of the Anti Financial Crime Head Office Department are described in its Organizational Code and in the "IICS Regulation".

The Anti Financial Crime Head Office Department, in a capacity as Anti-Money Laundering Function:

- is independent from the operational entities since it reports to the Chief Compliance Officer Governance Area and has enough resources to carry out its duties from a qualitative and quantitative standpoint;
- reports directly to Senior Management;
- has access to all business activities, as well as significant information for carrying out its duties.

The Anti Financial Crime Head Office Department monitors risks of money laundering, terrorist financing and breach of embargoes, carrying out the following activities:

- defining the guidelines, methodological and processes to adopt for risk management;
- monitoring the risk assessment process, contributing to its integration in the Risk Appetite Framework (RAF) and planning management actions;
- monitoring the regulatory alignment process, guaranteeing that external regulations are monitored at all times and adequately translated into guidelines, rules, processes and internal procedures;
- advising and assisting Corporate bodies and other Bank entities on interpreting and adopting internal and external regulations, and assessing conformity to applicable regulations in advance (clearing) for innovative projects, including the start of new activities and entry on new markets, new products and services to market and sensitive transactions;

- establishing the control objectives to mitigate risk, cooperating with other company entities in defining first and second level controls, and reviewing the results to define and monitor mitigation actions;
- assisting in disseminating an adequate risk culture at all levels of the company;
- managing relations with the Supervisory Authorities and nonconformities;
- preparing periodic reports for Corporate Bodies;
- monitoring specific obligations concerning i) customer due diligence, ii) data retention, iii) monitoring transactions, iv) reporting suspicious transactions and (iv) managing risk in a non-EEA context;
- guiding, coordinating and controlling Subsidiaries without centralised management and Foreign Branches.

With specific reference to customer due diligence obligations, the Anti Financial Crime Head Office Department carries out the following activities:

- prepares and updates the rules and methods and supports the drafting of the operating processes relating to profiling methods, customer identification and due diligence (standard and enhanced);
- assesses and authorises new accounts, occasional transactions or the continuation of accounts already held for high risk customers, save for any activities assigned by the Head of the Anti Financial Crime Head Office Department to other Bank entities, based on objective, previously established criteria;
- assesses and authorises the opening of new accounts, occasional transactions or the continuation of existing accounts for medium risk positions, in relation to a specific request from operating entities, as well as cases where personnel in charge of the assessment or authorisation are in situations of even potential conflict of interest;
- assesses customers found to be on the Sanctions Lists when registering or updating their personal data, if identified by the automatic control systems and confirmed following the checks carried out by the competent Operations Head Office Department;
- prepares and certifies the standard questionnaire relating to the internal processes and procedures adopted by the Bank on anti-money laundering, combating terrorist financing and managing embargoes, to generally be delivered to banks or financial institutions that carry out due diligence for new bank accounts or similar relationships with the Bank.

With specific reference to obligations to retain data, the Anti Financial Crime Head Office Department carries out the following activities:

- defines the data archive input and management requirements, to comply with anti-money laundering obligations, and checks the reliability of the information system used for data entry, based also on controls carried out by other company entities. More specifically, the Anti Financial Crime Head Office Department provides assistance in the phase involving analysis of IT activities on said archive and coordinates activities to eliminate any anomalies identified in its management;
- controls, on a random basis, the quality of statistical data to send to the FIU and coordinates adjustments, considered necessary, to information recorded in the relative archive (also following requests from operating entities);
- sends aggregate data on the above records to the FIU each month.

With specific reference to obligations on transactions monitoring, the Anti Financial Crime Head Office Department carries out the following activities:

- prepares and updates the transaction monitoring methods for anti-money laundering, anti-terrorism and embargo management purposes;
- within the scope of managing embargoes, carries out assessments (and oversees the authorisation, as applicable) of transactions ordered by/in favour of customers who are on the Sanctions Lists, on the basis of automatic filtering and following checks carried out by the competent entities of the Operations Head Office Department;

- sends the FIU periodic objective communications in accordance with implementing provisions issued by the FIU.

With specific reference to obligations on reporting suspicious transactions, the Anti Financial Crime Head Office Department - through the Head of Suspicious Activity Reporting - carries out the following activities:

- reports to the FIU on transactions considered as second level suspicious with respect to money laundering, terrorist financing or the financing of programmes for the proliferation of weapons of mass destruction;
- manages obligations related to access of the Authorities, in particular the FIU and Finance Police.

With specific reference to periodic reporting and information flows for Corporate Bodies, the Anti Financial Crime Head Office Department:

- every six months, prepares and submits a report to the Board of Directors on controls carried out, actions taken, shortcomings identified, corrective measures to be taken and personnel training;
- analyses any findings on offences pursuant to Articles 46, paragraph 1, letter b), and 51, paragraph 1, of Legislative Decree no. 231/2007, sent by the Chief Audit Officer and/or other company functions, and provides the relative disclosure, on a half-yearly basis, to the Management Control Committee; if there are particularly serious offences, this disclosure will be given at the next applicable meeting to ensure that timely communication is given to the Supervisory Authorities or the Ministry of Economy and Finance;
- takes note of the reports pursuant to Articles 46 and 51 of Legislative Decree no. 231/2007, forwarded by the Management Control Committee to the Supervisory Authorities, the Ministry of Economy and Finance, or the Head of Suspicious Activity Reporting and reports to the Management Control Committee on the corrective actions taken.

With specific regard to personnel training, the Anti Financial Crime Head Office Department carries out the following activities:

- identifies the training objectives and prepares an adequate training programme to ensure that the employees are kept constantly up to date, together with the Compliance, Governance and Controls Head Office Department, the Development Policy and Learning Academy Head Office Department and the People Management & HR Transformation Head Office Department;
- defines the content of training activities and supports the Development Policy and Learning Academy Head Office Department and the People Management & HR Transformation Head Office Department in deciding on how the activities should be carried out.

In the Anti Financial Crime Head Office Department:

- the Head of Anti Financial Crime Head Office Department is given the position of the Head of the Anti-Money Laundering Department;
- the Head of Suspicious Activity Reporting and Authorisations of the Anti Financial Crime Head Office Department is given the position of Head of Suspicious Activity Reporting.

4.3.1.1 Head of the Anti-Money Laundering Function

The Head of the Anti Financial Crime Head Office Department is given the position of Head of the Anti-Money Laundering Function, as approved by the Board of Directors.

The Head of the Anti Financial Crime Head Office Department:

- must comply with suitable independence, authority and professional competence requirements and must not have direct responsibilities over operating areas, nor report to the persons in charge of said areas;
- is considered, for all intents and purposes, as one of the heads of the corporate control functions and performs his/her functions independently;

- receives a periodic information flow relating to reports forwarded and filed from the Heads of Suspicious Activity Reporting of the Parent Company and Group Companies and may request to examine reports forwarded and filed[4];
- carries out a supervisory role on the adequacy of the organisation of activities and actual implementation of the internal processes and procedures with respect to anti-money laundering, combat of terrorist financing and managing embargoes within the scope of all the company units, even if said units do not belong to the Anti Financial Crime Head Office Department. In carrying out that role, and for the applicable profiles, shares the first level control activities to be carried out with applicable operational, business and control entities and their implementation procedures;
- uses the results of the second level controls carried out by the applicable units that belong to his/her Department and the Compliance Governance and Controls Head Office Department, and the results that emerge from controls carried out by the Chief Audit Officer entities as part of the third level independent control function;
- monitors the adequacy of internal processes and procedures for the identification, assessment and reporting of suspicious transactions, as part of his/her duty to monitor the effectiveness of the entire management and internal control system overseeing the risk of money laundering, terrorist financing and breach of embargoes;

The Head of the Anti Financial Crime Head Office Department is also the Head of Anti-Money Laundering for main Companies of the Group where the centralised management model is adopted and, considering the steering, coordination and control role of the Parent Company as regards Group Companies, s/he is also the Group Head of Anti-Money Laundering, with overall management of money laundering risk at a Group level.

The Head of the Anti Financial Crime Head Office Department is delegated by the Managing Director and CEO to authorize the opening of cross-border accounts with correspondent banks or financial instructions in a non-EEA Countries and to authorise accounts or transactions with national and foreign Politically Exposed Persons, save for additional powers assigned by the Managing Director and CEO to other Bank entities.

The Head of the Anti Financial Crime Head Office Department reports directly to the Head of the Chief Compliance Officer Governance Area.

4.3.1.2 Head of Suspicious Activity Reporting

The Head of AML Suspicious Reporting and Authorisations of the Anti Financial Crime Head Office Department is given the position of Head of Suspicious Activity Reporting, as approved by the Board of Directors.

The Head of AML Suspicious Reporting and Authorisations:
- must comply with suitable independence, authority and professional competence requirements and must not have direct responsibilities over operating areas, nor report to the persons in charge of said areas;
- exercises his/her functions independently;
- also holds the position of Group Delegate, with authority to forward reports of suspicious activity to the FIU, also on behalf of Group Companies that adopt the centralised management model;
- has free access to the information flows addressed to Corporate Bodies and to other entities involved in activities to combat money laundering and terrorist financing;

[4] With reference to the Foreign companies of the Group, the circulation of analytical information on the reports sent to local FIUs takes place unless there are any obstacles provided under the legal system of the country where the Foreign Company of the Group in question has its head office.

- may acquire from the Head of the Anti Financial Crime Head Office Department information that can help to assess suspicious activity;
- may allow, taking necessary measures to ensure confidentiality and without mentioning the reporting party's name, the Heads of corporate units to know the names of reported customers, given the particular significance that this information may have for the purpose of accepting new customers or assessing existing customers transactions;
- provides operating entities with advice on obligations regarding the preparation of suspicious transaction reporting and possible abstention from performing transactions;
- assesses the suspicious activity reports received from the operational entities and the communications forwarded to it pursuant to Article 46, paragraph 1, letter a) of Legislative Decree no. 231/2007 by the Management Control Committee, and prepares the related preliminary inquiry;
- sends reports considered to have grounds to the FIU;
- files reports considered as unfounded, providing reasons in writing;
- communicates the outcome of his/her assessment to the Head of the operational entity from which the report originated, notifying the Head of the Anti Financial Crime Head Office Department through periodic information flows or as requested;
- after being informed, notifies the Head of the operating entity reporting the suspicious transaction that the inquiry has been filed as instructed by the FIU;
- liaises with the FIU and manages requests for further inquiries submitted by the competent authorities[5];
- contributes to identifying the measures necessary to guarantee the confidentiality and retention of data, information and documentation relating to reporting to be submitted for approval by the Managing Director and CEO.

The Head of AML Suspicious Reporting and Authorisations, in carrying out his/her duties, is assisted by staff of the Suspicious Activity Reporting entity; in particular, s/he may enable the above personnel to work, under his/her responsibility, on the suspicious activity reporting system, in compliance with instructions from the FIU.

4.3.2 Compliance Governance and Controls Head Office Department

The duties and responsibilities of the Compliance Governance and Controls Head Office Department are described in its "Organizational Code".

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Compliance Governance and Controls Head Office Department assists the Anti Financial Crime Head Office Department, ensuring the following:

- second level control activities for the Parent Company and Subsidiaries with centralised management;
- processing the indicators to monitor the higher risk events identified in accordance with the Anti Financial Crime Head Office Department.

4.3.2.1 Risk Assessment and Coordination of Compliance Initiatives

The duties and responsibilities of Risk Assessment and the Coordination of Compliance Initiatives are described in its "Organizational Code".

With specific reference to anti-money laundering, combating terrorist financing and managing embargoes, Risk Assessment and Coordination of Compliance Initiatives assists the Anti Financial

[5] The term Authorities refers to institutional bodies such as magistrates, the finance police and its special currency unit which may be involved in the inquiry and further investigation stages following suspicious reports from the financial system.

Crime Head Office Department in developing the AML Risk Assessment methods and monitoring the training implemented at Banks and Companies with centralised management.

4.4 Chief Risk Officer Governance Area

The duties and responsibilities of the Chief Risk Governance Area and entities reporting directly to him/her are described in the "Organizational Code", and "IICS Regulation".

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Chief Risk Officer Governance Area carries out the following activities:

- works with the Head of the Anti Financial Crime Head Office Department, who operates in accordance with the Head of the Chief Compliance Officer Governance Area, for the definition of the risk assessment methods relating to money laundering, terrorist financing and breach of embargoes encouraging synergy with the Operational Risk Management instruments and methods;
- works with the Head of the Anti Financial Crime Head Office Department, that operates in accordance with the Head of the Chief Compliance Officer Governance Area, to integrate the model to assess and manage compliance risk in the Risk Appetite Framework;
- supports the units of the Chief Compliance Officer Governance Area, through the Anti Financial Crime Head Office Department, in assessment of the compliance with prevailing laws on transactions and new products and services to put onto the market, also with reference to starting up new activities and entering new markets, both upon request, and through a structured clearing process, helping to identify the potential risks for the Bank and the Customers, and providing, where applicable, quantitative assessments.

The procedures for collaboration between the Chief Risk Officer and Chief Compliance Officer Governance Areas and related information flows are set out in the "IICS Regulation".

4.5 Chief Audit Officer

The duties and responsibilities of the Chief Audit Officer are described in the "Organizational Code", and in the "IICS Regulation".

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Chief Audit Officer, as part of third level controls of the overall internal control system, monitors the degree of adequacy of the corporate organisational structure and its compliance with applicable laws on an ongoing basis, and also oversees the functioning (in terms of efficiency and effectiveness) and reliability of the Group risk management model. Specifically, the Chief Audit Officer inspects the adequacy and efficiency of the Anti Financial Crime Head Office Department at regular intervals and informs the competent Corporate Bodies of the outcome of his/her assessments.
The Chief Audit Officer, within the scope of his/her oversight activities, will ensure *inter alia*:

- constant compliance with due diligence obligations, when establishing customer accounts and during the relationship with the customer;
- the actual acquisition and ordered storage of the data and documents prescribed by applicable legislation;
- the correct functioning of the storage archive of the data and transactions carried out by the customers;
- the actual accountability of employees and business partners, and the managers of central and decentralised units in implementing all the requirements set out under applicable law.

Moreover, the Chief Audit Officer:

- in order to ensure enhanced control over the units that are most exposed to the risks of money laundering, terrorist financing and breach of embargoes, prepares, on the basis of the findings of the Audit Risk Assessment and the controls performed by the first and second level Functions, the control plan for all the operational entities involved;

- during audits, checks alignment between various management accounting procedures for customer transactions and the data entry and management procedure for the data archive required by anti-money laundering laws;
- informs the Anti Financial Crime Head Office Department and other Corporate Bodies of inefficiencies identified during auditing activities and suggests corrective measures to be taken;
- takes follow-up action to check that necessary corrective measures have been adopted and whether they are suitable for preventing similar critical aspects in the future.

Following the controls and assessments performed, the Chief Audit Officer:

- identifies the possible offences pursuant to Article 46, paragraph 1, letter b), and Article 51, paragraph 1 of Legislative Decree no. 231/2007 and reports them to the Anti Financial Crime Head Office Department, for further analysis on its part, before forwarding the relative communication to the Management Control Committee;
- sends, on a confidential basis, to the Head of the operational entity, the communication to promptly start up the necessary assessments to initiate the reporting procedure for transactions identified as potentially suspicious in accordance with Article 46, paragraph 1, letter a) of Legislative Decree no. 231/2007. At the same time, the Head of Suspicious Activity Reporting is informed.

4.6 Chief Operating Officer Governance Area

4.6.1 Organisation Head Office Department

The duties and responsibilities of the Organisation Head Office Department are described in its “Organizational Code”.

The Organisation Head Office Department carries out the following activities:

- establishes organisational solutions in line with the objectives and strategies for anti-money laundering, combating terrorist financing and managing embargoes, advised and assisted by the Anti Financial Crime Head Office Department;
- checks and defines, with the approval of the Head of the Chief Operating Officer Governance Area, staff numbers, in line with the objectives and strategies of company plans;
- assists the Anti Financial Crime Head Office Department in updating these Guidelines, establishing planned roles and responsibilities;
- monitors the dissemination of internal regulations and the Bank's governance documentation on anti-money laundering, combating terrorist financing and managing embargoes.

In particular, the Organisation Head Office Department monitors the analysis and adoption of organisational measures, also arising from new regulatory obligations.

4.6.2 Development Policies and Learning Academy Head Office Department

The duties and responsibilities of the Development Policy and Learning Academy Head Office Department are described in its “Organizational Code”.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Development Policy and Learning Academy Head Office Department carries out the following activities:

- cooperates, with the units of the Chief Compliance Officer Governance Area and in particular with the Anti Financial Crime Head Office Department in the development of initiatives aimed at disseminating, at all levels of the company, a company culture that is consistent with the principles of compliance with law, and expanding the level of awareness of the possible resulting risks;
- works with the People Management & HR Transformation Head Office Department to carry out training initiatives on compliance, assisted by Chief Compliance Officer Governance Area

entities and especially with the Anti Financial Crime Head Office Department, which prepares the contents;
- works with the People Management & HR Transformation Head Office Department and with the Chief Compliance Officer Governance Area entities and especially with the Anti Financial Crime Head Office Department to define and develop training programmes on an ongoing basis, in order to further technical/professional expertise and update personnel tasked with compliance activities.

4.6.3 People Management & HR Transformation Head Office Department

The duties and responsibilities of the People Management & HR Transformation Head Office Department are described in its “Organizational Code”.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the People Management & HR Transformation Head Office Department will ensure the proper qualitative-quantitative workforce cover needed to meet regulatory obligations.

4.6.4 Labour Affairs and Policies Head Office Department

The duties and responsibilities of the Labour Affairs and Policies Head Office Department are described in its “Organizational Code”.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Labour Affairs and Policies Head Office Department:
- assesses and oversees disciplinary actions to be taken against employees who have breached regulations;
- assesses the applicability of the protections established by the collective contracts in the interests of employees involved in criminal, civil and administrative proceedings for alleged breaches of the applicable law and decides on the formulation of the concerns to be resolved when settling the proceedings.

4.7 Business Units and other operational, business and support functions

The Business Units[6] and the other operational, business and support functions have the primary responsibility for managing risks of money laundering, terrorist financing and breach of embargoes: During daily operations, these structures must identify, measure or assess, monitor, and mitigate and report the risks arising from ordinary company operations in accordance with the risk management process set out in the "IICS Regulation"; they must also comply with the operational limits assigned to them in accordance with the risk objectives and the procedures underlying the risk management process.

The operational, business and support functions comply with the company processes and procedures, checking its application with adequate first level controls in order to ensure that the transactions are carried out properly, for the full and complete compliance with applicable rules and standards of conduct. The operational and business entities, in association with the Anti Financial Crime Head Office Department and the Compliance Governance and Controls Head Office Department define the first level controls that they believe are capable of actually achieving the control objectives, and then implement them, involving the Organisation Head Office Department and Transformation Center for areas in their responsibility. The first level controls identified by the

[6] At the date of going to press, the Business Units comprised: the Banca dei Territori Division, the Corporate and Investment Banking Division, the International Subsidiary Banks Division, the Private Banking Division, the Asset Management Division and the Insurance Division.

operational, business and support functions are submitted for review by the Anti Financial Crime Head Office Department and the Compliance Governance and Controls Head Office Department, that will assess their capacity to actually achieve the control objectives, and if necessary, will request their consolidation.

The operational, business and support functions have a significant role in monitoring risks from money laundering, terrorist financing and the violation of embargoes. For this purpose, they put in place all initiatives aimed at encouraging the diffusion of a culture of compliance with operators, working with them to correctly implement the training programmes defined by the Anti Financial Crime Head Office Department in accordance with the Chief Compliance Officer Governance Area entities, in association with applicable corporate functions. Also:

- the control entities of the Banca dei Territori Division, Corporate and Investment Banking Division and Private Banking Division, as well as the NPE Synthesis and Controls Function of the Credit Governance Head Office Department, in line with service and organisational current models, are responsible for ensuring that operating entities under their responsibility comply with obligations, reporting any shortcomings identified and requesting remedial actions. The result of the checks carried out and any shortcomings found will be communicated to the Chief Compliance Officer Governance Area units and the Chief Audit Officer for the assessments that they are responsible for;
- the operational and business entities, in line with current service and organisational models, play an active role meeting the requirements of various regulatory frameworks and governed by specific guidelines, processes and internal procedures.

The operational, business and support entities play an active role in meeting requirements relating to anti-money laundering, combating terrorist financing and managing embargoes. More specifically, for the purposes of customers' knowledge, the entities carry out the following activities:

- identify customers as well as beneficial owners, obtain information and documents (including additional information necessary in the case of relations with banks and financial institutions), necessary to carry out the due diligence obligations and assign the customer risk profile;
- increase the risk profile associated with the customer, where necessary, up to a medium risk, based on evidence produced by profiling instruments and propose any increase to a high risk to the Anti Financial Crime Head Office Department;
- take an independent decision on whether to refuse to open an account or execute an occasional transaction for medium risk customers, involving the Anti Financial Crime Head Office Department, if considered appropriate;
- retain documents obtained and keep relative information updated;
- monitor customer accounts and transactions steadily;
- inform the customers of the Bank's decision not to open an account and/or execute a transaction or of its intention to close an existing account.

Lastly, the operating structures carry out the following activities:

- identify breaches in regulations concerning limitations in the use of cash and bearer-negotiable instruments promptly notifying them to the Ministry of Economy and Finance, and sending a copy of the communication to the Anti Financial Crime Head Office Department;
- check *in advance* payments and documents representative of goods, to ensure they conform to provisions of the Anti Financial Crime Head Office Department as regards transactions with Countries, goods sectors or entities subject to sanctions and/or restrictions;
- check in advance payments ordered by/in favour of customers to verify that they do not have links with the lists of entities known as "Bad Guys", since they are considered to be high-risk on the basis of the profiles assigned by the Group;
- carries out checks, through the function that reports to Head of the line control operational entity, to ensure that the monitoring of transactions and assessment of offences in terms of limitations on the use of cash or bearer-negotiable instruments are properly undertaken.

4.8 Other Structures

4.8.1 Legal Affairs Head Office Department - Group General Counsel

The duties and responsibilities of the Legal Affairs Head Office Department – Group General Counsel are described in the "Organizational Code".

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Legal Affairs - Group General Counsel Head Office Department carries out the following activities:

- supports the Anti Financial Crime Head Office Department in identifying steadily applicable laws, monitoring developments, including case law developments, and providing legal advise to ensure the correct and unique interpretation within the Group;
- shares, for legal aspects within its area responsibility, the contents of these Guidelines, internal regulatory provisions and training courses prepared by the Anti Financial Crime Head Office Department and other assigned entities, formulating proposals for amendments and/or additions;
- advises and assists the Anti Financial Crime Head Office Department on controversial legal aspects concerning the compliance assessment of internal processes and procedures, contracts, forms or significant cases of inefficiencies that have been identified;
- shares, with the Anti Financial Crime Head Office Department, standard drafts of notices to be sent to customers regarding the refusal to open an account, or closing of an account or refusal to carry out an occasional transaction.

Criminal, Bankruptcy and Specialized Litigation and Civil Litigation units as well as the International Advisory and Litigation unit, each for its own area of expertise and responsibility, manage pre-litigation and litigation cases related to money laundering, terrorist financing and embargoes.

4.8.2 Transformation Center

The duties and responsibilities of the Transformation Center are described in its "Organizational Code".

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Transformation Center carries out the following activities:

- assists the process owner in planning company processes and monitoring updates to and the publication of internal regulations on anti-money laundering, combating terrorist financing and managing embargoes;
- identifies, jointly with the Anti Financial Crime Head Office Department and functions involved, the requirements to develop the most suitable IT solutions to simplify the applicable processes and increase their efficiency.

4.8.3 Operations Head Office Department

The duties and responsibilities of the Operations Head Office Department are described in its "Organizational Code".

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Operations Head Office Department carries out the following activities:

- cooperates, based on requirements of the Anti Financial Crime Head Office Department, in coordinating requests made to the IT Head Office Department, regarding activities on IT systems, apart from actions more closely related to anti-money laundering, combating terrorist financing or managing embargoes (e.g. systems for managing the data stored on customer accounts, identifying anomaly indicators, due diligence or risk profiling);

- performs first level controls on the quality of data entered in the data storage archive, addressing any requests for corrective measures to be taken to the IT Head Office Department and guaranteeing a periodic information flow to the Anti Financial Crime Head Office Department, with details of the anomalies found and the progress of corrective actions implemented;
- checks, based on the rules defined by the Anti Financial Crime Head Office Department, matches with the Sanctions List and/or the internal lists for anti-money laundering and embargo purposes (Bad Guys) resulting from automatic filtering systems and involving the Anti Financial Crime Head Office Department, if the suspicion is confirmed;
- checks, applying the rules defined by the Anti Financial Crime Head Office Department, payments and bills of lading if there is a match with the Sanctions List and/or the internal lists for terrorist financing combat and embargo purposes (Bad Guys), involving the Anti Financial Crime Head Office Department, if the suspicion is confirmed.

4.8.4 IT Head Office Department

The tasks and responsibilities of the IT Head Office Department are described in its “Organizational Code”.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the IT Head Office Department is involved in the development, update and monitoring of application components, carrying out the following activities, to this end:

- implements and maintains, on the basis of requirements defined by the Anti Financial Crime Head Office Department, the IT systems used to carry out the applicable obligations;
- controls the integrity and completeness of flows providing input for various application solutions used, with specific regard to the data retention archive to meet anti-money laundering obligations. In the event of anomalies, the IT Head Office Department activates the necessary corrective measures and informs the Anti Financial Crime Head Office Department;
- updates the Sanctions Lists, together with the Anti Financial Crime Head Office Department;
- implements the corrective measures indicated by the Anti Financial Crime Head Office Department and Chief Audit Officer.

4.8.5 Cybersecurity and Business Continuity Management

The duties and responsibilities of the Cybersecurity and Business Continuity Management unit are described in the “Organizational Code”.

The unit defines the rules and actions to take to protect the data, information and infrastructures to guarantee business continuity and the regular performance of company activities, and to keep security conditions in line with prevailing laws, also with reference to monitoring anti-money laundering, combating terrorist financing and managing embargoes.

4.8.6 Institutional Affairs Head Office Department and International Public Affairs

The duties and responsibilities of the Institutional Affairs Head office Department and the International Public Affairs entity are described in their “Organizational Code”.

With reference to managing the risk of money laundering, terrorist financing and breach of embargoes, the Institutional Affairs Head Office Department and International Public Affairs unit monitor the evolution of the rules that are significant for the Group, informing internal entities and coordinating the Group's response to debate concerning proposed legislation.

5. MACRO-PROCESSES FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING AND FOR MANAGING EMBARGOES

The following main macro processes were identified, which describe how to monitor and control the risk of money laundering, terrorist financing and breach of embargoes:

- definition of guidelines and methodological rules;
- risk assessment and risk appetite framework;
- planning of activities;
- regulatory alignment;
- advisory and clearing;
- assurance;
- diffusion of a culture on anti-money laundering, combating terrorist financing and managing embargoes;
- interaction with the Authorities and management of non-compliance events;
- specific requirements;
- information flows to Corporate Bodies.

5.1 Definition of guidelines and methodological rules

The Head of the Anti Financial Crime Head Office Department, in accordance with the Head of the Chief Compliance Officer Governance Area, defines the applicable guidelines and methodological rules to monitor and assess, at Group level, the risk of money laundering, terrorist financing and breach of embargoes.

The operational and reputational components of the risk assessment methods, and the way to integrate the assessment of such risk into the Risk Appetite Framework are defined by the Head of the Anti Financial Crime Head Office Department, in accordance with the Head of the Chief Compliance Officer Governance Area and with the help of the Head of the Chief Risk Officer Governance Area.

5.2 Risk Assessment and Risk Appetite Framework

The identification and periodic assessment of the risk and related vulnerability constitutes the first logical step in the management model, and helps in the definition of the risk appetite principles and consequent limits to submit for approval to the Board of Directors within the scope of the Risk Appetite Framework (RAF), and identification and programming of the actions to take to reduce risk in the area of money laundering, terrorist financing and breach of embargoes.

The Bank of Italy Regulation of 26 March 2019 with implementing provisions on organisation, procedures and internal controls requires recipients to carry out an overall assessment, which is periodically updated, of its exposure to money laundering risk to indicate in the Annual Report (the so-called self-assessment of exposure to the risk of money laundering).

The Head of the Anti Financial Crime Head Office Department annually formulates a risk assessment on money laundering, terrorist financing and breach of embargoes (the AML Risk Assessment) for main entities of each Division and for the Group, which it submits to the Risk Committee, the Management Control Committee and Board of Directors. This assessment is drawn up on the basis of the records provided by the Anti Financial Crime Head Office Department (for the Italian Banks and Companies of the Group that apply the centralised management model) and by the AML Officers of Group Companies and Foreign Branches (that apply the steering, coordination and control model).

The assessment is carried out on the basis of the methods defined by the Head of the Anti Financial Crime Head Office Department, in accordance with the Head of the Chief Compliance Officer Governance Area and with the help of the Head of the Chief Risk Officer Governance Area. In particular, the AML Risk Assessment methodology surveys the extent of inherent risk and related vulnerabilities, through mainly quantitative indicators, integrated with qualitative assessments that relate the types of potential risk (e.g. customer risk level, risk level associated with non-cooperative Countries for the purposes of Commission Delegated Regulation (EU) 2019/758) and aspects mitigating the risk of money laundering, terrorist financing and breach of embargoes (e.g. the number of customers whose beneficial owner has been recorded), in relation to the dimensional data of the entity in question.

The risk assessments at Division level result from aggregation of the assessments of the relevant entities of each Division with the Group assessment from the aggregation of the assessments of the Divisions. The assessment of the inherent risk, the vulnerability and the residual risk is expressed on a four-level scale, which is the same as the other Corporate Control Functions.

The risk assessment models with respect to money laundering, terrorist financing and breach of embargoes are integrated into the RAF. To this end, within the scope of defining the RAF, the Head of the Anti Financial Crime Head Office Department, in accordance with the Head of the Chief Compliance Officer Governance Area:

- proposes qualitative statements relating to the risk of money laundering, terrorist financing and breach of embargoes;
- shows the risk profiles resulting from the AML Risk Assessment and proposes related risk appetite levels;
- establishes the limits relating to the operating losses and other relevant quantitative Key Risk Indicators to monitor the risks, with a specific focus on those which could constitute indicators of breaching the law in the area of financial crime; if the established thresholds are exceeded, the causes are identified and analysed and the steps to mitigate them are defined, implementing, where necessary, the escalation mechanisms provided by the Guidelines on the RAF;
- identifies, in accordance with their sensitivity, any specific risk categories with respect to money laundering or terrorist financing, where it is necessary to separately asses the risk level and defines specific management guidelines, monitoring and mitigation actions;
- defines the way to assess and control reputational risks resulting from the breach of mandatory regulations or self-regulation.

The AML Risk Assessment evaluations also contribute to the Integrated Risk Assessment - prepared within the scope of the Controls and Operational and Reputational Risk Coordination Committee, Integrated SCI session - aimed at providing a summarised viewpoint of the assessments produced by each Control Function on the Group as a whole, and on the main legal entities and operational, business and support functions, in accordance with the methods in use with each function.

5.3 Planning of activities

The identification and prior assessment of risks of money laundering, terrorist financing and breach of embargoes and related vulnerabilities is prior to the planning of management interventions, which are submitted, in the context of annual anti-money laundering reports, to the Board of Directors for approval, after review by the Risks Committee and Management Control Committee.

The Head of the Anti Financial Crime Head Office Department plans management interventions annually. Planning of activities is carried out considering all activities to implement, allocated by macro-processes and defined in terms of priorities, objectives, times and relative use of human and financial resources. If any shortcomings are identified, reported by resources, suitable mitigations actions are defined according to risk-based logics, and notified to the competent Corporate Bodies.

5.4 Regulatory alignment

The monitoring of the risk of money laundering, terrorist financing and breach of embargoes is carried out on a preventive basis, firstly ensuring that external laws are constantly monitored and adequately incorporated into the guidelines, processes and internal procedures. The regulatory alignment is guaranteed through the following activities:

- the continued identification and interpretation of the external regulations that apply to the Bank, through continuous monitoring of the external regulatory sources, and the consolidation, if there are changes in the law, of a single, agreed interpretation;
- assessment of the impact of applicable regulations on company processes and procedures, with proposed organisational and procedural modifications aimed at ensuring an adequate control of risks.

The Anti Financial Crime Head Office Department is in charge of continually identifying external laws, with the support of the Legal Affairs Head Office Department - Group General Counsel in order to interpret the laws.

The assessment of the impact of applicable laws and consequent proposal of guidelines, rules, processes and procedures is managed by the Anti Financial Crime Head Office Department, with assistance from the Organisation Head Office Department and Transformation Center, and for legal aspects, from the Legal Affairs Head Office Department - Group General Counsel.

The purpose of regulatory alignment is to define *ex ante* a framework for compliance with regulations and laws, based on the following guidelines:

- the guidelines and main strategies to manage the areas with crossover impacts on Group operations are defined in specific guidelines that need to be approved by the Board of Directors;
- the rules governing relevant areas are set out in documents that describe the methodological aspects, operational mechanisms, rules of conduct and mandatory restrictions to comply with, also implementing the guidelines and in compliance with the policies contained therein;
- the processes, where standardised, are supported by IT procedures and instruments that can assist and guide the behaviour of the staff, in order to ensure they behave correctly;
- in the more sensitive processes, the guidelines and rules of other Bank structures provide for the prior involvement of the Anti Financial Crime Head Office Department;
- the processes establish a system of controls which can effectively monitor the effectiveness of the controls over time, even taking into account the legal and business evolution.

5.5 Advisory and clearing

Compliance risk monitoring adopts a preventive-based approach, also through the following activities:

- the advisory activity and assistance given to Corporate Bodies and Bank structures on the interpretation and application of external and internal rules;
- the prior assessment of compliance with prevailing laws (clearing) on:
  - innovative projects, including the start up of new activities and entry on new markets, identifying for the latter the Countries where any new establishment would imply a risk considered to be unacceptable;
  - new products and services to be marketed and/or significant changes to existing ones, in compliance with product governance principles;
  - sensitive cases and transactions in relation to which company processes, as governed by the guidelines and rules of other Bank structures, provide for the prior assessment by the Anti Financial Crime Head Office Department.

The Anti Financial Crime Head Office Department advises and assists Corporate Bodies and other company structures on issues concerning the actual application of external laws to company processes and activities, and the conduct to adopt.

With regard to clearing activities, the Anti Financial Crime Head Office Department analyses, inter alia, the compliance of corporate transactions identified as sensitive for the purpose of embargoes and that involve Countries, product categories, or parties subject to sanctions and/or restrictive measures.

The Anti Financial Crime Head Office Department also provides a binding opinion on anti-money laundering requirements where reputational risk arising from possible new entities of the Group established in Countries of interest is considered acceptable, identifying the Countries where any new establishment implies a risk considered to be unacceptable and for which a prior opinion from this Department is required

Controls are carried out by first level controls of business entities that, on a quarterly basis, check the actual adoption of measures which the binding opinion is based on. In the case of a negative opinion, the control will identify if the transaction has not been carried out.

The assessments of the Anti Financial Crime Head Office Department are carried out using formats that, as far as possible, are defined to include the following:

- the subject of the assessment;
- the applicable internal and/or external regulatory context;
- the main aspects to analyse, which are significant for assessment purposes;
- brief considerations, identifying the level of consistency with the spirit and letter of the law and internal regulations, any residual risks and recommendations.

The extent of the analysis is in proportion to the level of complexity and new aspects considered, as well as applicable regulations.

5.6 Assurance

5.6.1 The assurance model

The control of the risk of money laundering, terrorist financing and breach of embargoes, entails, also on a preventive basis, takes concrete form, in addition to a preventive perspective, through subsequent checks of the adequacy and effective application of the internal processes and procedures, the suggested organisational changes to prevent risk, and in general, the monitoring of effective compliance with external and internal rules by the company's entities.

In line with the Integrated Internal Control System Regulation provisions with respect to risk monitoring and control, the assurance model assigns:

- the line controls to the operational, business and support entities, carried out on a continuous basis over individual transactions, and the managerial analyses consisting of the systematic monitoring of phenomena characterised by high anomaly levels that have to be promptly dealt with, and/or reported to a context of operational and management uniformity;
- to level-two control functions the monitoring of the correct adoption - by operational, business and support entities - of the applicable methodological and control framework, through verifications on the design of processes, procedures and on the actual and correct adoption of required controls.

The model defined to create the risk assurance process relating to the risk of money laundering, terrorist financing and breach of embargoes provides for the following:

- during the definition of the review of company processes, also following changes to the external legal context, the Anti Financial Crime Head Office Department establishes the control objectives to mitigate the risk of money laundering, terrorist financing and breach of embargoes, notifying the operational, business and support structures, as well as competent organisational structure;

- the operational, business and support structures, in association with the Anti Financial Crime Head Office Department and the Compliance Governance and Controls Head Office Department define the first level controls that they believe are capable of actually achieving the control objectives, and implement them, involving the Organisation Head Office Department and Transformation Center for areas in their responsibility. The first level controls identified by the Divisions and other operational, business and support structures are submitted for review by the Anti Financial Crime Head Office Department and the Compliance Governance and Controls Head Office Department, that will assess their capacity to actually achieve the control objectives, and if necessary, will request their consolidation;
- the Anti Financial Crime Head Office Department and Compliance Governance and Controls Head Office Department, on the basis of an assessment of the process defined in that manner and the results of the first level controls, will define and carry out the second level controls; these controls may be remote, checking the performance of monitored events, or on-site controls of processes adopted by operating structures and their effectiveness, as well as controls on the correct performance of level-one controls by operating structures; depending on the level of risk identified, and taking account of capacity limits , the frequency of controls may be continual or periodic, or inter-annual, annual, or long-term, or on a *una tantum* basis.

5.6.2 Method for carrying out activities

The continuous and periodic first level controls and second level controls are formalised, in accordance with the provisions of internal corporate rules, in specific control charts that identify the unit in charge, the objective and how the control is carried out, the relative frequency, the criteria to use to attribute the results of the control and how it is reported.

The *una tantum* second level controls, mostly relating to checks on the processes and/or phenomena considered to be significant, are planned by the Compliance Governance and Controls Head Office Department, in association with the Anti Financial Crime Head Office Department, on an annual basis, taking account of the results of the AML Risk Assessment and/or other signs (for example findings by the Supervisory Authorities or the Chief Audit Officer units, specific requests of the Corporate Bodies).

The Compliance Governance and Controls Head Office Department reports these controls to the Anti Financial Crime Head Office Department and to the operational, business and support structures; this reporting must be based on a format defined beforehand, as far as possible, and must include:

- the characteristics of controls (the subject, the applicable internal/external regulatory context);
- details of controls carried out and relative outcomes;
- brief considerations, indicating residual risks and mitigation actions suggested.

Individual organisational units are responsible for planning and adopting corrective actions; the above-mentioned Head Office Departments monitor and track the progress of actions identified.

5.6.3 Interaction with other control functions and information flows

The collaboration methods between the Corporate Control Functions and the relative information flows are set out in the "IICS Regulation".

In carrying out the checks, the Anti Financial Crime Head Office Department and the Compliance Governance and Controls Head Office Department also use the results of checks by the Chief Audit Officer units, who make the necessary assessments on the processes and behaviour, making the relative results available to the units in charge of monitoring.

Additionally, in order to ensure the ongoing effectiveness and validity of the control systems monitoring the risks of money laundering, terrorist financing and breach of embargoes, specific

Groups have been set up at Divisional level, where considered necessary, in which the first, second and third control level Functions take part, to:

- get more in-depth information on the findings from the control activities, encouraging the standard and integrated assessment of the risks in question;
- analyse the results of the assessments made by the Supervisory Authorities;
- share and coordinate the remediation actions to put in place to deal with the most significant anomalies found, monitoring their execution;
- plan the activities related to implementation and update of the control system in terms of preparation and reviewing the relative internal rules, identification of any procedural adjustments and definition of the consequent information flows in order to set up the control activities on a consistent and integrated basis.

The Anti Financial Crime Head Office Department and the Compliance Governance and Controls Head Office Department have access to all the Bank activities and any relevant information to carry out their duties, including through direct interaction with the staff. To this end:

- they receive and send the information flows reported in the "IICS Regulation";
- the other company structures must inform them, in a timely and complete manner, of any relevant facts in order to monitor the risks in question;
- they may request and receive any other relevant information to carry out their duties from the other company functions.

5.6.4 Follow-up process

The development of risk mitigation actions to solve criticalities identified by assurance controls and compliance with relative deadlines are followed up on a continual basis by the Anti Financial Crime Head Office Department through specific mechanisms defined, based on the significance of the criticalities and supported by adequate tools to monitor the progress of individual activities and evolution of gaps identified, in order to take necessary escalation initiatives, in the case of significant delays.

5.7 Diffusion of a culture on anti-money laundering, combating terrorist financing and embargoes

The diffusion, at all company levels, of a culture based on the principles of honesty, fairness and compliance in accordance with the spirit and letter of the law is a basic assumption in controlling risk. The effective adoption of regulations on money laundering, combating terrorist financing and managing embargoes must bear in mind the aims and principles underlying the system.

The Anti Financial Crime Head Office Department works with the Development Policies and Learning Academy Head Office Department and the People Management & HR Transformation Head Office Department to establish efficient channels of communication and training instruments, identifying relative training requirements and preparing the content of training initiatives for all the Bank resources, in order to ensure that staff, with specific attention paid to the sales staff and the heads of the business structures, have adequate awareness of applicable laws, obligations and related responsibilities, the consequences resulting from failure to fulfil said obligations and to ensure they are able to knowingly use supporting instruments and procedures in meeting requirements established by law.

The Anti Financial Crime Head Office Department, with the assistance of the Development Policies and Learning Academy Head Office Department and the People Management & HR Transformation Head Office Department monitors development of the training programmes, checking its use and effectiveness, and provide adequate results to the Corporate Bodies, also for the timely identification of any action that may need to be taken.

In addition to traditional training activities, the Anti Financial Crime Head Office Department, guided by the Group Control Coordination and Operational and Reputational Risk Committee, and in association with the Development Policies and Learning Academy Head Office Department, organises and takes part in specific initiatives aimed at disseminating a culture of risk and expanding the level of awareness of the approach to risk requested, including in particular:

- induction sessions for Company Bodies and workshops for senior management on particularly delicate or topical issues;
- actions to make the operational, business and support structures more aware of the specific risk aspects involved in ordinary operations;
- diagnostic activities in order to understand the level of diffusion of the risk culture at all company levels, in terms of consistency of perceptions and conduct with respect to required guidelines and policies.

Specific training programmes are also provided for personnel of the Anti Financial Crime Head Office Department, to keep them up to date with relative developments, and specific induction sessions are held for AML Officers of the Group Companies and Foreign Branches on risks of money laundering, terrorist financing and breach of embargoes.

5.8 Interaction with the Authorities and management of non-compliance events

The management of relations with the Authorities and non-compliance events is an extremely important part of the control of compliance risk. The Anti Financial Crime Head Office Department provides for management of the following in the areas it is responsible for:

- relations with the Supervisory Authorities, coordinating activities necessary to follow up requests from the Authorities;
- non-compliance events, assisting and working with the unit involved, to ensure the identification and implementation of actions to take to bridge any organisational and/or procedural gaps.

Interaction processes also include sending specific reports to the Supervisory Authorities, in accordance with legal provisions on anti-money laundering, combating terrorism and managing embargoes. This reporting includes:

- the monthly transmission of aggregate data concerning archive records to the FIU;
- the transmission of suspicious transaction reporting to the FIU;
- sending the Financial Intelligence Unit (FIU) and the special unit of the Finance Police communications relating to the freezing of funds and economic resources related to parties to whom restrictive measures apply, within the scope of laws on embargoes and combating terrorist financing;
- sending the Financial Intelligence Unit (FIU) periodic communications regarding transactions at risk in accordance with the implementation provisions issued by the Financial Intelligence Unit (FIU).

5.9 Specific requirements

5.9.1 Customer Due Diligence

Customer due diligence requirements are commensurate with the assessment of the actual level of risk of money laundering and terrorist financing associated with the customer. The risk of money laundering and terrorist financing is assessed considering the customer's characteristics, conduct and the specific nature of the account or transaction to carry out, taking into account the criteria indicated in applicable legislation.

Based on the level of risk attributed to the customer, the following approach to due diligence is adopted:

- ordinary obligations;
- simplified obligations;
- enhanced obligations.

Due diligence obligations shall be observed (i) in relation to accounts and transactions that are part of institutional activities, ii) in all cases where money laundering or terrorist financing is suspected, regardless of any exception, exemption or applicable threshold and (iii) when there are doubts as to the accuracy or adequacy of data previously obtained.

If it is not possible to comply with customer due diligence obligations, an account cannot be opened, a transaction cannot be carried out, or an assessment of whether to close an existing account must be made. In these cases, the sending of suspicious activity reporting must be considered.

Customer due diligence obligations are met through:

- identifying the customer, any executing party and beneficial owners, and checking the identity of these subjects: the identification is based on obtaining identification documents, documents certifying due diligence issued by other intermediaries and any additional information required to establish the risk profile to be assigned to the customer; assessing the identity of subjects based on documents, data and information obtained from a reliable and independent source;
- customer profiling based on the risk of money laundering, terrorist financing and breach of embargoes: profiling is based on assigning a score - produced from data and information obtained when opening an account and monitoring activities - and the consequent classification of customers into four bands, depending on whether the risk is considered as high, medium, low or insignificant; in the case of medium or high risk customers, enhanced due diligence obligations apply; profiling is subject to a harmonisation process at a Group level, based on which each Company of the Group undertakes the highest risk profile from those assigned by other Group Companies for the same customer[7];
- authorisation to open a new account, execute an occasional transaction or maintain an existing account on the basis of the risk profile assigned to the customer: for high or medium risk customers, to whom enhanced due diligence obligations apply, authorisation is issued: (i) for high risk customers, by the Anti Financial Crime Head Office Department, save for any authority given by the Head of this Department to other Bank structures, based on previously established, objective criteria; (ii) for medium risk customers, by the operating structure. With reference to Politically Exposed Persons, an authorisation procedure is started with specific authorisation from a senior manager based on specific authority issued by the Managing Director and CEO;
- authorisation or refusal to proceed, issued by the Anti Financial Crime Head Office Department, for customers, who, during the collection of information or updates of the register, are found to be on the Sanctions Lists, also following checks carried out by the applicable functions of the Operations Head Office Department;
- the periodic update of information on customer due diligence and periodic review of the risk profile: for customers with a high or medium risk, data on due diligence are updated, and the relationship is reviewed, every 18 and 24 months[8], apart from Politically Exposed Persons, whose data and banking relations are reviewed every 18 months, regardless of the risk associated with the customer; besides this frequency, the following events require the classification of subjects with a high or medium risk and, if the score increases, the updating of data on due diligence and a review of the position: i) acquiring the status of Politically Exposed Person; ii) reporting suspicious activity; iii) notification of a criminal investigation.

---

7 If a Group Company allocates a lower risk profile than that allocated by the other Group Companies, the reasons for this must be specifically justified in writing.

8 The foregoing is without prejudice to different review periods approved by the Bodies of Subsidiaries and Foreign Branches of the Group.

Under no circumstances may due diligence obligations be assigned to shell banks or intermediaries established in high risk third Countries[9] or whose local laws prevent adequate monitoring of the risks of money laundering or terrorist financing and, in particular, the sharing of data and information relative to own customers, within its own group.

5.9.1.1 Ordinary due diligence obligations

For customers without a high or medium profile related to risk of money laundering and terrorist financing, classified as having an immaterial or low risk, ordinary due diligence obligations apply, consisting in identifying the customer, any executing party and beneficial owner, checking the identity of subjects referred to, based on documents, data and information obtained from a reliable, independent source, and obtaining and assessing information for this purpose and on the nature of the ongoing relationship or occasional transaction, and carrying out continuous controls on the account/relationship.

5.9.1.1.1 Remote transactions

Remote transactions, meaning transactions carried out without a physical presence at the receiver of the customer, of employees or other personnel appointed by the receiver, require specific measures in carrying out due diligence, also considering the risk of fraud related to identity theft.

In this regard, the Bank:

- obtains identifying data regarding the customer and any executing party and their correspondence on a copy - obtained by fax, post, in an electronic format or with similar procedures - of a valid identity document pursuant to applicable legislation; and
- obtains additional information, concerning the process of identifying the customer, according to a risk-based approach, through one or more of the following measures: (i) telephone contact on a land line (welcome call), (ii) sending notices to a physical address with notification of receipt, (iii) transfer made by a customer through a banking and financial intermediary established in Italy or an EU member country, (iv) a signed request to send documents, (v) checks on residence, domicile, activities carried out, through requests for information from competent offices or through meetings on site, with own or third-party personnel, (vi) findings based on solutions with secure forms of biometric recognition.

Alternatively, risk mitigation takes place by identifying the customer/natural person remotely, according to the audio/video registration procedure governed in the Bank of Italy Regulation of 30 July 2019, with implementing provisions on customer due diligence.

5.9.1.2 Simplified customer due diligence

In the case of a low or insignificant risk of money laundering or terrorist financing, due diligence obligations may be simplified, reducing the extension and frequency of ordinary obligations. This category, unless otherwise determined ad hoc regarding a specific customer, comprises the following customer categories:

- banking and financial intermediaries as indicated in Article 3, paragraph 2 of Legislative Decree 231/2007, excluding traders, insurance intermediaries operating in the life sector, trust companies registered pursuant to Article 106 of the Consolidated Banking Act, financial advisors and financial consulting companies as indicated in Articles 18-bis and 18-ter of the Consolidated Finance Act;
- companies listed on regulated markets and subject to the disclosure obligations that include ensuring adequate transparency of beneficial owners;

[9] Listed in the Commission Delegated Regulation (EU) 2016/1675, as amended.

- public administrations, institutions or bodies that perform public functions conforming to European Union law;
- banking and financial intermediaries in the EU or with their headquarters in a non-EEA country adopting an effective system to combat money laundering and terrorist financing, based on indicators used to determine such risks.

Simplified due diligence entails the following, in any case:
- collecting information necessary to identify the customer, any executing party and beneficial owner, and to check their identity;
- with reference to the beneficial owner, reconstructing the control chain, based on the customer's declaration or on reliable external sources;
- obtaining information on the scope/nature of the account/relationship, also using assumptions in identifying whether the product is intended for a specific use;
- collecting all other information necessary for customer profiling, also using information that may be inferred from public sources (institutional sites of the Supervisory Authorities, sites of intermediaries involved, financial statements where available, external info providers);
- carrying out continual control of account/relationship;
- retaining data and information on accounts and transactions, according to previously established procedures.

The simplified fulfilment of the due diligence obligations is subject to continuous verification of the persistence of the relevant conditions.

Simplified due diligence does not apply when:
- there are doubts, uncertainties or inconsistencies regarding identifying data and information obtained during identification of the customer, any executing party or the beneficial owner;
- the conditions to adopt simplified due diligence no longer apply, based on the risk indices in applicable legislation;
- the monitoring of overall transactions of the customer and information obtained exclude a low risk of money laundering and terrorist financing;
- in any case, when money laundering or terrorist financing is suspected.

5.9.1.3 Enhanced customer due diligence

Enhanced due diligence applies to customers classified as high risk, in medium or high risk range. The following are always considered as high risk:
- particular types of accounts and transactions:
  - accounts and occasional transactions involving high-risk third Countries[10];
  - correspondent accounts that involve payments, and similar accounts with credit and financial institutions established in a non-EEA country;
  - cash transactions with large denomination bank notes;
  - transactions with unusually high amounts, or for which there are doubts as to their purpose;
  - deposits of cash/instruments from other States;
- special types of customers:
  - Politically Exposed Persons;
  - other types of customers considered as high risk, such as: entities that only trade gold, trusts, Italian and foreign money transfer companies that undertake cash remittances, agents in Italy and abroad of Italian and Foreign Financial Institution, Money Transfer Institutions that undertake cash remittances, customers concerned with the disbursement of public funds/awarded public contracts, betting operators, customers that are members of the System for the Protection of Applicants of Asylum and Refugees (SPRAR), trust

[10] Listed in the Commission Delegated Regulation (EU) 2016/1675, as amended.

companies that are not part of the Intesa Sanpaolo Group, regardless of whether they are registered in the register of trustees pursuant to Article 106 of the Italian Consolidated Banking Act, foreign financial or credit intermediaries not subject to the authorization to carry out the" activities by the Supervisory Authorities of the country where the principal place of business is established.

Enhanced due diligence measures entail:

- collecting further information on:
  - the customer, any executing party and the beneficial owner or the ownership and control structure in order to check data and minimal information, including the acquisition and assessment of information concerning reputation of the customer and beneficial owner;
  - the account/relationship to fully understand its nature and scope, obtaining information on the nature of activities carried out by the customer and/or beneficial owner, the allocation of funds, the reasons for which the customer requires a given product/service;
- a greater frequency and intensity of continual controls of accounts, with the updating of information and profiling, the examination of significant transactions or anomalies and overall movements, also based on types of amounts or transactions not considered by automatic monitoring or aggregation procedures;
- checking the origin of funds of the customer, used in accounts;
- adopting a specific authorisation procedure, which is stricter than that ordinarily used, when opening the account or performing the transaction. In particular for accounts and transactions with customers that are Politically Exposed Persons, as well as correspondent accounts with banks or financial institutions having their principal place of business in non-EEA Countries, specific authorisation by a senior executive is required, based on specific authority granted by the Managing Director and CEO.

5.9.2 Record keeping

To retain the identifying data of customers and data on accounts/relationships set up and transactions carried out, information is entered in the Unique Electronic Archive (AUI); this archive is managed by the Anti Financial Crime Head Office Department and by the IT Head Office Department, each to the extent of their responsibility, in order to ensure the clarity and completeness of the information that it is filed, that must be easy to consult. On the basis of this archive, the aggregate data concerning the operations of the Bank are sent, on a monthly basis, to the Financial Intelligence Unit (FIU) by the Anti Financial Crime Head Office Department,

To meet obligations to retain data, the following are also kept:

- the copy of or references to documents required for due diligence, for a period of ten years from when the account is closed;
- documents and records on transactions and accounts, comprising original documents or copies that provide an equivalent evidence of proof in legal proceedings, for ten years from when the transaction is carried out or the account is closed.

5.9.3 Transactions monitoring

Transactional monitoring obligations are met through the ongoing control of accounts, in order to verify the consistency of transactions with the scope of the account declared by the customer, identifying any transactions that are "unexpected", anomalous or inconsistent with the economic and financial profile of the customer or any news of significant events concerning the customer.

Three main processes have been established to guarantee control of transactions carried out by customers:

- *ex ante* monitoring, by the operational structures that carry out the transactions, to identify, block or report those suspected of money laundering, terrorist financing or breaching regulations on embargoes, and regarding the limitations of use of cash and bearer-negotiable instruments. The

operating structures may be assisted by the advisory entity that reports to the Head of Suspicious Activity Reporting to assess whether there are grounds to refrain from carrying out a transaction. If there are grounds, the operating structures notify the Head of Suspicious Activity Reporting, so that s/he may assess whether to not carry out the transaction and request the FIU to issue a suspension measure in case of evident risk;

- *ex ante* control of the payments and documents representing goods by checking them against the Sanctions Lists and/or the internal Group lists (Bad Guys) and checking the findings from the control procedures. These checks first involve the Operations Head Office Department and the operating structures that perform the transactions, which, if necessary, require authorisation from the Anti Financial Crime Head Office Department to go ahead with the transactions;
- *ex post* monitoring of the transactions by the operational structures in order to identify anomalous transactions, including with the assistance of the automatic anomaly indicators management system (where provided for).

Furthermore, in order to reduce the risk of money laundering, terrorist financing and breach of embargoes, and the related reputational, legal and operational risks, taking into account specific regulations on the matter, the Intesa Sanpaolo Group (i) does not make "cover" payments[11] in United States Dollars and (ii) operates with payable-through accounts[12] only on condition that customer due diligence is guaranteed by the counterparty bank using said payable-through accounts[13].

5.9.4 Reporting of suspicious transactions

To ensure that obligations on reporting of suspicious transactions are met, the reporting procedure, in accordance with regulatory requirements, comprises two separate stages:

- first level reporting by the Heads of the company operational structures, who have to immediately report any transactions of this nature that they discover to the Head of Suspicious Activity Reporting;
- second level reporting by the company units identified in the Anti Financial Crime Head Office Department, who examine the reports received and, if considered warranted, send them to the Financial Intelligence Unit (FIU). Reports on transactions considered suspicious with respect to money laundering, terrorist financing or financing proliferation programmes for weapons of mass destruction coming from the operational structures fall under the above-mentioned examination.

With reference to other suspicious transactions identified by other company structures, the process comprises the following two stages:

- first level notification which is "highly sensitive" entered in the specific company procedure (IAR);
- second level notification, overseen by the company structure identified within the Anti Financial Crime Head Office Department, based on the obligation to report suspicious transactions that comes to its knowledge.

5.9.5 Risk management in a non-EEA Countries context

In compliance with provisions in the Commission Delegated Regulation (EU) 2019/758, which regulates the minimum action and type of additional measures to adopt to mitigate the risk of money

---

[11] Cover payments refer to the transfer of funds used when there is no direct relationship between the payment service provider of the payer and the beneficiary, so a chain of correspondence relationships has to be used between the payment service providers. A cover payment involves three or more payment service providers; this payment aims to provide financial coverage to a message sent by the payer's provider to the beneficiary's provider in which it gives direct communication of the transfer of funds.

[12] Payable-through accounts are cross-border correspondent banking relationships between financial intermediaries, used to carry out transactions in their own name and on the customers.

[13] In particular, under Legislative Decree no. 231/2007, in the case of a correspondent account with a non-EEA credit entity, the Bank must ensure that it has checked the identity of customers with direct access to transition accounts, that is has met customer due diligence obligations and, on request, may provide the data obtained in meeting such obligations.

laundering and terrorist financing in relation to non-EEA Countries, the Anti Financial Crime Head Office Department, in adopting Group methodologies, ensures that procedures of Group branches and units with their principal place of business in these non-EEA Countries are aligned with Group standards and allow for significant information on customers, including information on suspicious transactions to be shared, save for compliance with limits established by local legislation.

Where the legislation of non-EEA Countries does not allow Group branches and units established there to align with Group standards or to share significant information on customers with it, the Anti Financial Crime Head Office Department, in keeping with provisions in Commission Delegated Regulation (EU) 2019/758, informs the Bank of Italy and arranges for additional measures, according to a risk-based approach.

5.10 Information flows to Corporate Bodies

Processes for communication with Corporate Bodies provide for the following:

- disclosure on offences, pursuant to Article 46, paragraph 1, letter b), and Article 51, paragraph 1 of Legislative Decree no. 231/2007, sent to the Management Control Committee, on a half-yearly basis, or the next applicable meeting in the case of particularly serious offences; notice to the Supervisory Authorities or Ministry of Economy and Finance is only sent afterwards;
- a half-yearly report on controls carried out, actions taken, malfunctions identified and corrective measures to be taken as well as personnel training;
- a half-yearly report on training activities concerning anti-money laundering, combating terrorist financing and managing embargoes;
- specific information on issues of particular relevance.

6. GROUP GOVERNANCE

Considering its operational and territorial base, the Group systematically adopts a unified approach to anti-money laundering, combating terrorist financing and managing embargoes, with guidelines, rules, processes, controls and IT instruments that are reasonably standard at Group level. To that end, the Group Companies are required to adopt these Guidelines, adapting them to their company environment and, for the foreign companies, to their specific local regulations, and to submit them for approval by their Supervisory Body.

The strategic decisions taken at Group level concerning management of the risks of money laundering, terrorist financing and breach of embargoes are entrusted to the Parent Company's Corporate Bodies. The Corporate Bodies of the Group Companies must be aware of the choices made by the Parent Company's Corporate Bodies and are responsible, each for their own area of competence, for implementation of the strategies and policies for managing the risk of money laundering, terrorist financing and breach of embargoes in accordance with their business reality. In this context, the Parent Company involves, through the Group Head of the Anti-Money Laundering Function, the Corporate Bodies of the Group Companies, regarding the choices made with regard to policies, processes and procedures for managing the risk of money laundering, terrorist financing and breach of embargoes.

Within the Intesa Sanpaolo Group, specific duties assigned to the Anti-Money Laundering Function are carried out based on two separate models, which take account of the Group's operating and local structure. This process involves in particular:

- for specifically identified Italian Banks and Companies whose operations are highly integrated with the Parent Company, the centralisation of risk monitoring activities relating to money laundering, terrorist financing and breach of embargoes with the Anti Financial Crime Head Office Department (centralised management model). The choice to centralise the activities is backed by assessment and documentation of the risks, costs and benefits associated with it, in a Group logic; this analysis is regularly updated;
- for the other Companies where there is a regulatory obligation, and for foreign Branches, the establishment of an Anti-Money Laundering Function and appointment of a local AML Officer, as well as a Head of reporting suspicious activity, who are given responsibility for these matters (the steering, coordination and control model).

Italian Companies that have not been asked to establish an Anti Financial Crime Department, monitor relative risk within the scope of the Organisation, Management and Control Model pursuant to Legislative Decree no. 231/2001 assisted, for any specific matters, by the Anti Financial Crime Head Office Department.

In adopting the steering, coordination and control role of the Parent Company for Group Companies, the Anti Financial Crime Head Office Department works together with the business units, exchanging adequate information flows and maximising potential synergies. The International Subsidiary Banks Division in particular, works with the Anti Financial Crime Head Office Department in order to transpose and implement the guidelines and provisions issued by the Parent company into the individual foreign companies, relating to anti-money laundering, combating terrorist financing and managing embargoes, also taking account of the specific corporate context and the local regulations that apply.

6.1 The centralised management model

In Banks and Italian Companies where the centralised management model applies, the risk control activities with respect to money laundering, terrorist financing and breach of embargoes are carried out by the Anti Financial Crime Head Office Department of the Parent Company with the support of

the other units in the Chief Compliance Officer Governance Area. The activities provided are governed by specific agreements.

The Head of the Anti Financial Crime Head Office Department also acts as AML Officer for main Companies that apply the centralised management model. For other Banks and Companies with centralised management, the Head of the Anti Financial Crime Head Office Department appoints his representative as AML Officer, who is responsible for management of the risk of money laundering, terrorist financing and breach of embargoes on an outsourced basis, on behalf of the Bank or Subsidiary. The AML Officer is appointed from among executives or middle managers with adequate levels of professional expertise and experience for the role to be performed for each Bank or Company that outsources the activity, taking into account the related specific risks. The AML Officer is appointed subject to approval by the Supervisory Body of the Banks/Companies, after consulting with the Control Body.

Moreover, in compliance with the Bank of Italy Regulation of 26 March 2019, the Banks and Companies in question appoint an AML Reference person, who reports functionally to the designated AML Officer, assisting the Anti Financial Crime Head Office Department in carrying out its activities, with particular reference to the adoption of a specific company approach to policies to manage risks concerning money laundering, terrorist financing and breach of embargoes identified at a Parent Company level, the management of relations with Company Bodies and prompt reporting of events or particular situations, that may modify the risks generated by the subsidiary.

The AML Reference person shall:

- meet the necessary professional requirements;
- be positioned at a suitable hierarchical and functional level;
- not have direct responsibility for the operational areas subject to control or be hierarchically subordinate to the heads of those areas.

The AML Reference Person is appointed and removed from office by the Supervisory Body, after consulting with the Control Body, and subject to a prior opinion from the Head of the Anti Financial Crime Head Office Department.

With reference to potentially suspicious transactions, the operating entities of the Banks and Companies with centralised management promptly carry out first level reporting to the Group Delegate, that has authority to report suspicious transactions, as approved by the Supervisory Body, after consulting with the Control Body. Furthermore, the Company Control Bodies of Banks and Companies with centralised management notify the Group Delegate of any offences pursuant to Article 46, paragraph 1, letter a) of Legislative Decree no. 231/2007, identified during the exercise of its functions. The Group Delegate acquires, directly or through the Banks and Companies, information on the scope, including information in the data retention archive, to meet anti-money laundering obligations.

As regards breaches in Article 46, paragraph 1, letter b) and Article 51, paragraph 1 of Legislative Decree no. 231/2007, the control entities of the Banks and Companies with centralised management identify and report in time these breaches to the Anti Financial Crime Head Office Department that, through the Head of the Function and based on evidence from second level control activities carried out, informs the Control Bodies of Banks and Companies with centralised management in order to allow them to report to the Supervisory Authorities or Ministry of Economy and Finance; the above notification must also be made by Control Bodies when they identify offences while carrying out their own duties.

6.2 The direction, coordination, and control model

The Group Companies and Foreign Branches that adopt the steering, coordination and control model set up their own Anti-Money Laundering Function and appoint the relative AML Officer, that usually

holds the position of Head of Suspicious Activity Reporting: in Italian companies based on authority granted by the Supervisory Body, after consulting with the Control Body and in Companies and in Foreign Branches based on requirements of local legislation.

The AML Officer has an adequate hierarchical/functional position, i.e. reporting directly to the Management Body or Supervisory Body and reporting functionally to the Head of the Anti Financial Crime Head Office Department to implement the choices made by the Parent Company on policies, processes and procedures to manage risk concerning money laundering, terrorist financing and breach of embargoes. The appointment, withdrawal and incentives based on merit (in terms of defining objectives, appraising results and determining bonuses) of local AML Officers, shall receive a prior opinion from the Head of the Anti Financial Crime Head Office Department.

Besides carrying out the macro-processes established in these Guidelines, to monitor and control risks concerning money laundering, terrorist financing and breach of embargoes, the AML Officers of Group Companies and Foreign Branches that apply the steering, coordination and control model:

- inform the Anti Financial Crime Head Office Department, in full and as promptly as possible, about the outcomes of control activities carried out based on the control macro-objectives provided by the Head of the Anti Financial Crime Head Office Department, as well as any significant event. In this regard, it also provides half-yearly reports on issues governed by the guidelines set forth by the Parent Company[14];
- propose and/or share remedial actions to adopt for shortcomings identified, defining the relative times and responsibilities for implementation. In this regard, on a monthly basis, the Anti Financial Crime Head Office Department is notified of the progress of activities;
- work with the Supervisory Authorities in order to be updated on the regulatory framework and operate in compliance with applicable provisions relative to the business model adopted and/or Country of establishment, coordinating with the Anti Financial Crime Head Office Department, with a view to acting consistently with Guidelines and facilitating dialogue with the Authorities. The Anti Financial Crime Head Office Department assists the Group Companies and Foreign Branches in establishing relations with the Authorities, without prejudice to the responsibility of the individual Companies or Branches to implement the specific regulatory requirements of the business sector and/or country of residence;
- promptly informs the Anti Financial Crime Head Office Department if local laws do not permit the adoption of measures to combat money laundering, terrorist financing or to manage embargoes that are equivalent to those of the European Union, so that the Head of the Anti Financial Crime Head Office Department may inform the Bank of Italy pursuant to Legislative Decree no. 231/2007.

AML Officers are given responsibility for authorising the execution of an occasional transaction or for opening and continuing accounts with high risk customers and for assessing customers who are found to be on Sanctions Lists, during updates to records.

The Head of Suspicious Activity Reporting of Group Companies and Foreign Branches for which the steering, coordination and control model is applied, transmits to the Group Delegate a copy of suspicious activity reports sent to the FIU or to the competent Foreign unit,[15] and those filed, complete with motivation of said decision, without prejudice to local rules governing banking and/or professional secrecy, as well as any local provisions that prevent the transmission of these notices to the Group Delegate. The transmission of information is carried out using procedures designed to guarantee maximum confidentiality of the identity of the first level Manager making the report. In

[14] For example, these issues may concern developments in the local regulatory context, the number and type of transactions reported, the number and type of high risk customers accepted, training programmes scheduled and delivered, breaches of provisions found, objections received from the competent authorities.

[15] Article 33, paragraph 2 of Directive (EU) 2015/849 requires the party obliged to report the suspicious transaction to send information to the Unit of the Member State where it is situated.

order to investigate anomalous transactions and accounts at a Group level, the Group Delegate may be assisted by all Company structures.

The Anti Financial Crime Head Office Department sets out the Group guidelines and oversees their correct adoption by Companies and Foreign Branches that apply the steering, coordination and control model, according to procedures in these Guidelines. For this purpose, with reference to profiles related to the management of risks of money laundering, terrorist financing and breach of embargoes, the Anti Financial Crime Head Office Department:

- defines the Group guidelines and methodological rules, identifying the geographical and/or business scope of application and supporting its local implementation; These guidelines and methodological rules include, among others, the general principles or in any case minimum standards of conduct to adopt regarding:
  - due diligence obligations (information set and methods to carry out customer due diligence, and reviewing customer risk profiles and criteria for customer acceptance and abstention obligations);
  - obligations for the registration and retention of data (procedures for registration, retention and management of information and documentation acquired from customers);
  - processes and procedures to adopt for monitoring customer transactions;
  - processes and procedures to monitor activities concerning embargoes, with particular reference to the definition of Sanctions Lists and control objectives;
  - reporting obligations (procedures to assess potentially suspicious transactions in order to forward first level reporting, if applicable, and the timeliness of reporting, traceability of the assessment procedure and clear identification of responsibilities);
  - limitations on the use of cash and bearer-negotiable instruments:
  - training personnel (type of initiatives to deliver, minimum contents and users);
  - the controls system (control macro-objectives, type of and procedures for controls);
- assists the local AML Officers in producing risk assessments and analysing outcomes, in order to promote a uniform approach to assessments and achieve a global vision of risks and oversight at Group level, and in producing the annual steering, coordination and control plan according to a risk-based logic;
- defines - as part of project activities to manage risks concerning money laundering, terrorist financing and breach of embargoes of the Group - operating processes and relative supporting tools, coordinating the implementation stage at a local level;
- provides technical support to the Companies and Foreign Branches and activates the clearing process – at the discretionary request of any of the assessment structures at local level – engaging the competent entities of the Parent Company;
- guides the Companies and Foreign Branches in the development of uniform control methods and models, and assesses the adequacy and effective implementation of compliance controls established at Group level, also through on-site inspections;
- coordinates the training initiatives – checking their consistency and synergies with initiatives adopted at Parent Company level – and organising meeting days and/or events with local AML Officers;
- supports local AML Officers in responses to the Supervisory Authorities, helping to establish remediation plans and monitoring their implementation;
- supports local AML Officers, on request, in preparing information flows to Corporate Bodies.

To carry out its duties, the Anti Financial Crime Head Office Department has access to all activities of Group Companies and Foreign Branches in question, and to any significant information regarding risks of money laundering, terrorist financing and breach of embargoes, also through direct interviews with personnel.

The Group Companies and Foreign Branches that are subject to the steering, coordination, and control model, are required to:

- adopt, for Companies with approval from Corporate Bodies, guidelines and rules issued by the Parent Company on managing risks of money laundering, terrorist financing and breach of

embargoes, aligning them, where necessary, in coordination with the Anti Financial Crime Head Office Department, to their own context and specific aspects of local regulations;

- adopt the operating working standards and methods defined by the Anti Financial Crime Head Office Department, agreeing on any adaptations to reflect the specific situation of the company; more specifically, in the case of foreign subsidiaries, all the initiatives aimed at guaranteeing standards of control and monitoring that are similar to those provided by Italian supervisory provisions, also in the cases where the regulations of the Countries where the subsidiaries are located do not provide for similar levels of attention;
- give the Anti Financial Crime Head Office Department with reference to anti-money laundering, combating international terrorist financing and embargoes, the information flows defined in Attachment B of the Group Compliance Guidelines, also guaranteeing prompt information in the case of events that may cause the risks related to this sector to emerge.

The Group Companies that in turn directly or indirectly hold controlling interests, are required to identify the most suitable organisational models for the subsidiaries under their control, in agreement with the structures under the Anti Financial Crime Head Office Department. They are also responsible for ensuring that the guidelines issued by the Parent Company are distributed among the subsidiaries and verifying their correct adoption and application. The information flows sent to the Parent Company must provide suitable information on the compliance situation at subsidiaries, with reference to risks concerning anti-money laundering, combating terrorist financing and managing embargoes.