GUIDELINES FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING AND FOR THE HANDLING OF 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

Owner:
Anti-Money Laundering Head Office Department

Recipients:
Intesa Sanpaolo Group

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

Effective form: May 2018

INTESA SANPAOLO

CONTENTS

1. INTRODUCTION

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

These Guidelines identify the applicable standards, and define the risk management model with respect to money laundering, terrorist financing and breach of embargoes of Intesa Sanpaolo, setting out:

- the roles and responsibilities of the units involved;
- the macro-processes used to correctly identify, assess and manage said risks;
- the governance methods of Banks and Group Companies.

“Money laundering” refers to:

- 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 entails the use or concealing of criminal proceeds by persons who committed the crime that generated said proceeds (known as “self-money 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.

“Embargo” is defined as the ban on trade or 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 regulatory framework concerning anti-money laundering and combating terrorist financing

The main applicable laws for preventing and combating money laundering and terrorist financing can be divided into the following categories:

- European Union laws;
- primary and secondary Italian laws.

The main European Union laws are set out in the following directives:

- Directive (EU) 2015/849 of the European Parliament and Council of 20/05/2015 (the "IV Directive") on prevention of use of the financial system for the purpose of money laundering or terrorist financing, which amends (EU) regulation no. 648/2012 of the European Parliament and Council, and which revokes directive 2005/60/EC of the European Parliament and Council and directive 2006/70/EC of the Commission;
- Regulation (EU) 2015/847 of the European Parliament and Council of 20/05/2015 relating to the computer data that accompanies the transfer of funds and which revokes regulation (EC) no. 1781/2006;
- Delegated Regulation (EU) 2016/1675 (as amended by EU Regulations 2018/105 and 2018/212) supplementing the IV Directive identifying high-risk third countries with strategic deficiencies.

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

- Legislative Decree no. 231/2007, as amended by Legislative Decree no. 90 of 25/5/2017 which brought the Italian anti-money laundering regulatory framework in line with the new European provisions;
- Legislative Decree no. 109 of 22/6/2007, also as amended by Legislative Decree no. 90/2017, containing measures to prevent, combat and repress international terrorist financing, which imposes obligations to report frozen assets and resources and report suspicious activity.

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

- Communication dated 9 February 2018 which, pending the issue of new implementation provisions, identifies what sections of the previous measures by the Bank of Italy, listed below, continue to apply since they are compatible with the new primary regulatory framework;
- Regulation of 24 August 2010 containing the anomaly indicators for intermediaries in order to facilitate the identification of suspicious activity;
- Regulation of 10 March 2011 implementing rules for the organisation, procedures and internal controls to prevent the use of intermediaries or other entities performing financial activities for the purposes of money laundering or terrorist financing;
- Regulation of 3 April 2013 implementing provisions relating to customer due diligence, to the extent still compatible with Legislative Decree no. 231/2007;
- Regulation of 3 April 2013 implementing provisions for keeping the Single Electronic Archive and simplified registration procedures.

The regulations issued by US Authorities, included in the following main 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 in their financial institutions;
- US Patriot Act (Uniting and Strengthening America by Providing Appropriate Tool to Intercept and Obstruct Terrorism - 2001) which was issued following the terrorist attacks of 11 September 2001, extending the BSA requirements, and requiring financial institutions to prepare due diligence procedures and improve the sharing of information between the 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 Department 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.

Since it operates in New York, Intesa Sanpaolo signed the "US Patriot Act Certification" whereby its commercial and financial operations in the United States are also subject also to United States laws, such as the execution of payment orders in dollars and in general, transactional activities carried out on its own account and on the account 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 main principles of the regulatory environment are the following:

- the obligation to arrange risk prevention measures that are proportional to the type of customer, relationship, product or transaction. More specifically, it is necessary:
  - to acquire enough information to identify the customer, the beneficial owner and the scope of the relationship or the transaction;
  - constantly monitor the effectiveness of the relationship;
- 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 to report suspicious activity within the scope of active cooperation with the Authorities;
- the obligations regarding use of the cash, bearer securities or other means of payment;
- the obligation for adequate personnel training to ensure the correct application of the provisions;
- the obligation to store the data for anti-money laundering requirements;
- the obligation of the Control Body to report any relevant offences that it becomes aware of when carrying out its duties.

In order to comply with said obligations, the recipients must identify consistent organisational functions, resources and procedures that are in the right proportion to the type of activities carried out, their sizes, organisational complexity and operational characteristics.

The organisation required by the law must be based on:

- the setting up of a special function in charge of preventing and combating the execution of money laundering and terrorist financing transactions, the appointment of a person in charge and a person delegated the authority to report suspected money laundering or terrorist financing transactions;
- 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 the transactions;
- a control function structure with coordinated components, including through suitable information flows, and which is also consistent with the company size and complexity, the type of services and products offered as well as the degree of risk associated with the customers' characteristics;
- strong accountability by employees and outside business partners and suitable controls that can monitor their compliance with the regulatory obligations, the internal processes, and their implementation.

Finally, the regulations require Groups to guarantee the coordination of the controls on an efficient basis, for the prevention and combating of money laundering and terrorist financing, and to ensure

that the procedures in force at foreign companies and branches are in line with Group standards and ensure that information is shared at consolidated level.

These Guidelines shall comply with both European Union legislation and national legislation, and also with non-EU legislation where there are suitable links, without prejudice to compliance with the obligations established by the legal system of each country.

2.2 The regulatory framework concerning embargoes

The United Nations Charter grants the U.N. Security Council the power to make binding decisions for all United Nations Member States on restrictive measures aimed at keeping or restoring international peace and security. The Treaty of the European Union and the Treaty on the Functioning of the European Union provide that the member states should take a common position in the blocking or limiting of economic and financial relations with one or more third countries. The above-mentioned measures are designed to:

- safeguard the common values, fundamental interests, independence and integrity of the European Union in accordance with the principles of the United Nations Charter;
- strengthen the security of the European Union;
- preserve peace and strengthen international security;
- promote international cooperation;
- develop and consolidate democracy, compliance with law, and respect for human rights and fundamental freedoms.

The applicable laws for handling embargoes can be divided into the following categories:

- European regulations;
- primary and secondary Italian laws.

The main European Union laws are set out in the following directives:

- Regulation 2580/2001/EC of the European Council of 27/12/2001 that establishes an obligation to freeze capital and prohibits the provision of financial services to certain natural persons, legal persons, groups or entities that commit, or attempt to commit, any act of terrorism, or legal persons, groups or entities controlled by the foregoing;
- European Council Regulation 881/2002/EC of 27/5/2002, which imposes specific restrictive measures on certain persons and entities (listed in the attachment to the Regulation) associated with Osama bin Laden, the Al-Qaida network and the Taliban;
- European Council Regulation 428/2009/EC dated 5 May 2009 which sets up a European Union regime for the control of exports, transfer, brokering and transit of dual-use products (rewriting of the original Council Regulation 1334/2000/EC dated 22 June 2000, amended by Regulation 1382/2014 dated 22 October 2014);
- European Council Regulation (UE) no. 753/2011 of 1 August 2011, concerning further restrictive measures against certain persons, groups, enterprises and entities “in view of the situation in Afghanistan” and the decisions made by the “Sanctions Committee” and the “1267 Committee” established with the UN Security Council[1].

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 risk” countries, defined, within the scope of the company regulations, as “Category A countries”.

The primary Italian law is set out in the following decrees:

[1] The “Sanctions Committee” was established with the United Nations Security Council in accordance with point 30 of resolution 1988 (2011) of the UNSC, while the “1267 Committee” was established by the UNSC in accordance with resolutions 1267 (1999) and 1333 (2000) of the United Nations Security Council.

- Law no. 185/1990, as amended by Legislative Decree no. 105/2012 issued in implementation of Directive 2009/43/EC containing "New rules on the control of exports, imports and transit of weaponry". That law still forms the basis of the regulations on the transfer of goods classified as "weaponry";
- Legislative Decree no. 221/2017 which reordered and simplified the laws governing authorisation procedures for the export of dual-use products and technology, and the sanctions regarding commercial embargoes, and for all types of exports of proliferation materials. The regulations previously contained in Legislative Decree no. 11/2007, Legislative Decree no. 64/2009 and Legislative Decree no. 96/2003, revoked, were merged into that decree. The decree provides (articles 18 to 21) for application of criminal and administrative sanctions against those who export dual use goods in breach of the law.

With regard to the secondary regulations, the Bank of Italy Regulations mentioned above should be considered, and especially 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.

Also of particular significance, in view of the Intesa Sanpaolo Group operations in the United States, are the regulations issued by US Authorities, included in the "US Patriot Act" mentioned above as well as in the provisions relating to the economic and commercial sanctions decided by the US government as the occasion arises, through the Office of Foreign Asset Control (OFAC) within the scope of foreign policy and national security choices.[2]

The applicable regulatory framework, clearly similar to the one illustrated above with respect to money laundering and terrorist financing, provides for restrictive measures and sanctions with respect to both the governments of third countries and non-State entities, natural persons or legal persons relating to:

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

The applicable regulations require the Bank to provide for measures that guarantee:

- data registration and transactional controls on the transactions carried out by its customers and related to imports and/or exports;
- traceability of the checks carried out on transactions originating from/destined to countries, persons and entities against which restrictions have been established;
- the freezing of goods and resources that can be traced to designated parties that the restrictive measures apply to, and forwarding the resulting communications to the Financial Intelligence Unit (FIU);
- the reporting of suspected terrorist financing or weapons of mass destruction proliferation activities.

[2] At the date of publication of this document, the sanctions issued against Iran, Russia, North Korea, Syria and Venezuela fall into this area.

3. GENERAL GOVERNANCE MODEL PRINCIPLES

The Guidelines fall within the scope of the structure defined by the Group through the Integrated Internal Control System 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 10 March 2011 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 the 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;
- the 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 Business Units and other Operational and Business Functions comply with the company processes and procedures, checking application with adequate first level controls for the full and complete compliance with applicable regulations and standards;
- the Chief Audit Officer, within the scope of its ordinary activities, ensures ongoing monitoring of the degree of adequacy of the corporate organisational structure and its compliance with applicable laws and oversees the functionality 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:

- inspiration from the values of honesty, accuracy and responsibility; in substantive compliance with the Code of Ethics of the Group;
- cooperation with the Supervisory Authorities for the prevention of the issues in question, taking into account the regulatory provisions governing the confidentiality of reporting and information concerning suspicious activity, protection of personal data (privacy) and “banking secrecy”;
- adoption of oversight standards in terms of guidelines, rules, methods, processes and instruments in line with international principles and reasonably standard at Group level, in accordance with the applicable rules at local level;
- adoption of ‘risk-based’ control measures that are proportional to the characteristics and complexity of the activity performed and the legal form, size and organisational structure of the 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. The organisation of the tasks and responsibilities attributed to the Corporate Bodies of the Parent Company are set out in the relative Rules, and with reference to the internal control system, in the "Integrated Internal Control System Regulation".

4.2 Supervisory Board pursuant to Legislative Decree no. 231/2001

The duties and powers of the Board are described in the Organisation, management and control model pursuant to Legislative Decree no. 231/2001. The Supervisory Board, 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 the units reporting directly to it are described in its Organisational Code, the Integrated Internal Control System Regulation and the Intesa Sanpaolo Group Compliance Guidelines.

The Chief Compliance Officer ensures oversight of the risks of money laundering, terrorist financing and breach of embargoes, through the Anti-Money Laundering Head Office Department, which holds the role of "Anti-Money Laundering Function of the Parent Company" (hereinafter "Anti-Money Laundering Function") and through the Compliance Governance and Controls Head Office Department and the Coordination of Compliance Initiatives.

4.4 Anti-Money Laundering Head Office Department

The tasks and responsibilities of the Anti-Money Laundering Head Office Department are described in its Organisational Code and the Integrated Internal Control System Regulation.

The Anti-Money Laundering Function reports directly to the Chief Compliance Officer Governance Area Manager.

The following are allocated to the Anti-Money Laundering Function:
- the role of Head of the Anti-Money Laundering Function, attributed to the Head of the Anti-Money Laundering Head Office Department;
- the role of Head of Suspicious Activity Reporting, attributed to the Head of AML Suspicious Reporting and Authorisations of the Anti-Money Laundering Head Office Department.

Specifically, the Anti-Money Laundering Function:
- is a specialised second level control function;
- is independent from the operational units since it reports to the Chief Compliance Officer and has enough resources to carry out its duties from a qualitative and quantitative standpoint;
- reports directly to Senior Management;

- has access to all corporate activities as well as to any information relevant to the performance of its duties.

When defining and assessing the control over the risks of money laundering, terrorist financing and breach of embargoes, the Anti-Money Laundering Function also performs the following activities:

- supports the Chief Compliance Officer in the definition of the statements and limits of the Risk Appetite Framework;
- assesses the residual risk profile for money laundering, terrorist financing and breach of embargoes on the basis of the "AML Risk Assessment" method;
- monitors, with the assistance of the Legal Affairs Head Office Department - Group General Counsel, developments in the applicable national and international legislative framework, identifying applicable rules, assessing their impact on internal processes and procedures, proposing the necessary actions and ensuring they are put into place;
- assesses, beforehand (*ex ante*), for the applicable operating area defined within the scope of the relative guidelines, the compliance of new (i) processes, (ii) procedures, (iii) products, and (iv) services, and 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;
- identifies, in accordance with the applicable company units, the first and second level control objectives to attribute to the operational and business units;
- analyses the first level control results, the results of the second level controls carried out by the applicable units of the Chief Compliance Officer Governance Area, analyses the inefficiencies found and the corrective measures indicated by the Chief Audit Officer units;
- continuously checks the company processes and procedures on the basis of the information received from the control units, and proposes, in accordance with the applicable corporate functions, the organisational and procedural changes required and/or advisable to ensure adequate controls over the risk of money laundering, terrorist financing and breach of embargoes;
- manages, for the areas it is responsible for, relations with the Financial Intelligence Unit (FIU), the Bank of Italy, the Ministry of Economic Affairs and Finance and the Supervisory Authorities;
- provides, for its areas of responsibility, consultation and support to the Corporate Bodies and Senior Management;
- provides assistance and support to the central operational units and the territorial units of the Bank with regard to application of the law governing anti-money laundering, combating terrorist financing and handling embargoes;
- ensures control of the risks of money laundering, terrorist financing or embargo handling for Foreign Branches of the Parent Company and the companies managed on a centralised basis, where the AML Officers functionally report to the Anti-Money Laundering Function.

With specific regard to the prescribed customer awareness obligations, the Anti-Money Laundering Function performs 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 execution of due diligence (standard and enhanced);
- assesses and authorises, pursuant to Article 25 of Legislative Decree no. 231/2007, the opening of new accounts, the execution of occasional transactions or the maintenance of existing accounts for customers assigned as high risk, or for medium risk customers when a specific request is submitted by the operational units;
- assesses and authorises the opening of new accounts, executing occasional transactions or the maintenance of existing accounts for medium risk positions if the personnel in charge of the assessment or authorisation find themselves in situations of even potential conflict of interest;
- assesses customers who are found to be included in the Sanction Lists when registering their personal data or updates the data register, if identified by the automatic control systems and confirmed following the checks carried out by the applicable 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 embargoes handling matters, to generally be delivered to banks or financial institutions that carry out the due diligence to initiate correspondent banking relationships or similar relationships with the Bank.

With specific regard to the registration obligations, the Anti-Money Laundering Function performs the following activities:

- defines the data input and storage file management requirements to comply with the anti-money laundering obligations, and checks the reliability of the information system used for data entry, based also on controls carried out by other corporate units. More specifically, the Anti-Money Laundering Function provides assistance in the phase involving analysis of IT activities on said archive and coordinates activities to remove any anomalies found in its management;
- makes sample checks of the quality of the statistical data to send to the Financial Intelligence Unit (FIU) and coordinates the amendments, considered necessary, to the information recorded in the relative file (also following the request by the operational units);
- sends the aggregate date relating to the above-mentioned registrations to the Financial Intelligence Unit (FIU) every month.

With specific regard to the obligations relating to the awareness of the transactions, in addition to the activities for which the Head of Suspicious Activity Reporting is responsible, the Anti-Money Laundering Function performs the following activities:

- prepares and updates the transaction monitoring methods for anti-money laundering, anti-terrorist and embargo handling purposes;
- examines and keeps copies of the reports on breaches of regulations concerning limitation of use of cash and bearer securities, forwarded by the operational units to the Ministry of Economic Affairs and Finance;
- within the scope of the handling of embargoes, makes the applicable assessments (and authorises any execution) of transactions ordered by/in favour of customers who are on the *Sanction Lists,* both on the basis of automatic filtering and following checks carried out by the applicable units of the Operations Head Office Department;
- sends the Financial Intelligence Unit (FIU) periodic communications regarding transactions at risk in accordance with the implementation provisions that will be issued by the Financial Intelligence Unit (FIU).

The Anti-Money Laundering Function also guarantees periodic reporting and direct information flows to the Corporate Bodies and Senior Management. Specifically:

- every six months, it prepares and submits a report on the inspections carried out, actions taken, shortcomings found and corrective measures to be taken and personnel training activities to the Board of Directors;
- it 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 Economic Affairs and Finance. Communications in accordance with article 46, paragraph 1, letter a) of Legislative Decree no. 231/2007 relating to potential suspicious activity are also communicated to the Head of Suspicious Reporting and Authorizations of the Anti-Money Laundering Head Office Department;
- 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 Economic Affairs 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-Money Laundering Function performs the following activities:

- identifies the training objectives and prepares an adequate training programme to ensure that the employees are kept constantly up to date, in association with the Coordination of Compliance Initiatives, the Development Policy and Learning Academy Head Office Department and the People Management & HR Transformation Head Office Department;
- defines the content of the 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 they should be run.

4.4.1 Head of the Anti-Money Laundering Function

The role of Head of the Anti-Money Laundering Function is attributed to the Head of the Anti-Money Laundering Head Office Department, by resolution of the Board of Directors.

The Head of the Anti-Money Laundering Function:

- must comply with suitable independence, authority and professional competence requirements and must not have direct responsibilities over operating areas and must not be obliged to report to the persons in charge of said areas;
- is considered, for all intents and purposes, in the category of Heads of Corporate Control Functions and executes his/her duties independently;
- also fulfils the role of Head of Group Anti-Money Laundering for the Group Companies for which application of the centralised management model is prescribed;
- receives a periodic information flow relating to reports forwarded and filed from the Heads of Suspicious Activity Reporting of the Parent Company and of the Group Companies and may request to examine reports forwarded and filed[3];
- 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 and handling of embargoes within the scope of all the company units, even if said units do not belong to the Anti-Money Laundering Head Office Department. In carrying out that role, and for the applicable profiles, shares the control activities to be carried out with the applicable Business Unit units (first level control) and their implementation procedures;
- uses the results of the second level controls carried out by the applicable units that belong to its Department and the Compliance Governance and Controls Head Office Department, and the results that emerge from the assessments carried out by the Chief Audit Officer units in its third level independent control function;
- monitors the soundness of the internal processes and procedures for recognition, assessment and reporting of suspicious activity since it is in charge of monitoring the effectiveness of the whole management and internal control system overseeing the risk of money laundering, terrorist financing and breach of embargoes.

The Head of the Anti-Money Laundering Function is given, by Managing Director and CEO, in its capacity as General Manager, the delegation to authorise/pursue the opening of ongoing relationships with Politically Exposed Persons - foreign PEPs or high risk resident PEPs, and correspondent banking accounts, payable through accounts, and similar accounts with credit or financial institutions located in non-equivalent third countries pursuant to Article 25 of Legislative Decree no. 231/2007; this is subject to any delegation of authority attributed by the Managing Director and CEO to other Bank Units.

[3] With reference to the Foreign companies in the Group, the circulation of analytical information on the reports sent to the local FIU 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.

4.4.2 Head of Suspicious Activity Reporting

The role of Head of Suspicious Activity Reporting is attributed to the Head of Suspicious Reporting and Authorisations of the Anti-Money Laundering Head Office Department, which is delegated the authority, pursuant to Legislative Decree 231/2007, to act as legal representative of the Bank.

The Head of Suspicious Activity Reporting:

- must comply with suitable independence, authority and professional competence requirements and must not have direct responsibilities over operating areas and must not be obliged to report to the persons in charge of said areas;
- exercises its functions independently;
- also fulfils the role of Group Delegate, with assignment of the delegation of authority to forward reports of suspicious activity to the Financial Intelligence Unit (FIU), also on behalf of Group Companies for which application of the centralised management model is prescribed;
- has free access to the information flows addressed to the Corporate Bodies and the other units involved in combating money laundering and terrorist financing;
- may acquire from the Head of the Anti-Money Laundering Function information that can help it to assess the suspicious activity process;
- may allow, taking the necessary confidentiality precautions, and without mentioning the reporting party's name, the Heads of the corporate units to get to know the names of the reported customers, given the particular significance that this information may have for the purpose of accepting new customers or assessing existing customers' operating activity;
- provides the operational units with advice on obligations regarding preparation of suspicious activity reports and possible abstention from performing transactions;
- assesses the suspicious activity reports received from the operational units 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 the Financial Intelligence Unit (FIU) the reports deemed to be founded;
- files the reports deemed not to be founded providing written reasons;
- communicates the outcome of its assessment to the Head of the operational unit from which the report originated, notifying the Head of the Anti-Money Laundering Function through the prescribed periodic information flows or in response to its request;
- notifies the Manager of the operational unit that made the suspicious transaction report that the report prepared by the Financial Intelligence Unit (FIU) was filed when it becomes aware of this;
- liaises with the Financial Intelligence Unit (FIU) and manages requests for further investigation submitted by the competent Authorities[4];
- contributes to identification of the measures needed to guarantee the confidentiality and storage of the data, information and documentation relating to the reports to be submitted for approval by the Managing Director and CEO.

The Head of Suspicious Activity Reporting, in carrying out its duties, is assisted by staff skilled in Reporting Suspicious Activities; more specifically, it may enable the employees of said unit to work, under its responsibility, in the suspicious activity reporting system in accordance with the instructions issued by the Financial Intelligence Unit (FIU).

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

4.5 Compliance Governance and Controls Head Office Department

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

With reference to the matters relating to anti-money laundering, combating terrorist financing and handling embargoes, the Compliance Governance and Controls Head Office Department assists the Anti-Money Laundering Function, ensuring the following:

- second level control activities for the Parent Company and the subsidiaries to which the centralised management model applies;
- steering, coordination and control with respect to the Subsidiaries where the centralised management model does not apply;
- processing the indicators to monitor the higher risk events identified in accordance with the Anti-Money Laundering Function;
- reporting with respect to the Corporate Bodies.

4.6 Coordination of Compliance Initiatives

The duties and responsibilities of the Coordination of Compliance Initiatives are described in its Organisational Code.

With specific reference to the matters relating to anti-money laundering, combating terrorist financing and handling of embargoes, the Coordination of Compliance Initiatives assists the Anti-Money Laundering Function in developing the AML Risk Assessment methods and monitoring the training implemented in the Banks and Companies on the centralised management model.

4.7 Chief Risk Officer Governance Area

The tasks and responsibilities of the Chief Risk Officer Governance Area are described in its Organisational Code and the Integrated Internal Control System Regulation. With respect to the control over the risks of money laundering, terrorist financing and breach of embargoes, the Chief Risk Officer Governance Area performs the following activities:

- works with the Head of the Anti-Money Laundering Function, who operates in accordance with the Chief Compliance Officer Governance Area Manager, 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-Money Laundering Function, which operates in accordance with the Chief Compliance Officer Governance Area Manager, to integrate the model to assess and manage the risk of non-compliance into the Risk Appetite Framework;
- supports the units of the Chief Compliance Officer Governance Area, through the Anti-Money Laundering 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 cooperation procedures between the Chief Risk Officer Governance Area and the units of the Chief Compliance Officer Governance Area and relative exchanges of information are set out in the Integrated Internal Control System Regulation.

4.8 Chief Audit Officer

The tasks and responsibilities of the Chief Audit Officer are described inits Organisational Code and the Integrated Internal Control System Regulation.

It is the Chief Audit Officer's duty to carry out third level independent controls, including with respect to combating money laundering, terrorist financing and handling of embargoes.

The Chief Audit Officer, within the scope of its ordinary activities, ensures ongoing monitoring of the degree of adequacy of the corporate organisational structure and its compliance with reference laws and oversees the functionality of the entire internal control system. Specifically, it regularly inspects the adequacy and efficiency of the Anti-Money Laundering Function and informs the competent Corporate Bodies of the outcome of its assessments.

The Chief Audit Officer, within the scope of its oversight activities, will ensure *inter alia*:

- constant compliance with due diligence obligations, when establishing customer accounts and in the course of 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 for 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.

Also:

- 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 units involved; this is 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;
- checks, during the auditing, alignment between the various management accounting procedures for the transactions carried out by customers and the data entry and management procedure for the storage archive of the data provided for under anti-money laundering laws;
- informs the Anti-Money Laundering Function and other Corporate Bodies of the deficiencies detected during the checking activities and recommends corrective measures to be taken;
- performs follow-up activities to ensure that the necessary corrective actions have been taken and that they can ensure that similar critical situations can be avoided 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-Money Laundering Function, for further analysis on its part, before forwarding the relative communication to the Management Control Committee;
- sends, on a confidential basis, to the Operational Unit Manager, the communication to promptly start up the necessary assessments to initiate the reporting procedure for the transactions identified as potentially suspicious in accordance with article 46, paragraph 1, letter a) of Legislative Decree no. 231/2007. At the same time, inform the Head of Suspicious Activity Reporting of this.

4.9 Chief Operating Officer Governance Area

4.9.1 People Management & HR Transformation Head Office Department

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

With regard to combating the phenomena of money laundering, terrorist financing and breach of embargoes, the People Management & HR Transformation Head Office Department will ensure the proper qualitative-quantitative workforce cover needed to fulfil the obligations under the law.

4.9.2 Labour Affairs and Policies Head Office Department

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

With regard to combating the phenomena of money laundering, terrorist financing and breach of embargoes, the Labour Affairs and Policies Head Office Department:

- assesses and promotes disciplinary actions with respect to employees who have not fulfilled the obligations set out under applicable laws;
- 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 address when settling the proceedings.

4.9.3 Development Policies and Learning Academy Head Office Department

The duties and responsibilities of the Development Policies and Learning Academy Head Office Department are described in its Organisational Code.

With respect to controlling the risks of money laundering, terrorist financing and breach of embargoes, it carries out the following activities:

- cooperates, with the units of the Chief Compliance Officer Governance Area, in the development of initiatives aimed at spreading, at all levels of the company, a company culture that is consistent with the principles of compliance with the law, and expanding the level of awareness of the possible risks resulting from that;
- works with the People Management & HR Transformation Head Office Department to implement the training on compliance, with support from the Chief Compliance Officer Governance Area units, and to the extent applicable, the Specialised Functions, who prepare the content.

4.10 Business Units and other operational and business functions

The Business Units[5] and the other operational and business functions have the primary responsibility for management of the risks of money laundering, terrorist financing and breach of embargoes: during the course of their daily operations, these units must identify, measure or evaluate, monitor, mitigate and report on the risks arising from ordinary business operations, in accordance with the risk management process set out in the “Integrated Internal Control System Regulation”, they must also comply with the operational limits imposed upon them by the risk objectives and the risk management processes.

The Business Units and other organisational units comply with the company processes and procedures, checking 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 standards of conduct. The operational and business units, in association with the Anti-Money Laundering Head Office Department, the Compliance Governance and Controls Head Office Department and the Chief

[5] As at the date of publication of these Guidelines, the Business Units are: the Banca dei Territori Division, the Corporate and Investment Banking Division, the International Subsidiary Banks Division, the Private Banking Division, the Asset Management Division, the Insurance Division and the Capital Light Bank.

Operating Officer Governance Area define the first level controls that they believe are capable of actually achieving the control objectives, and then implement them. The first level controls identified by the Business Units and the other operational and business units are submitted for inspection by the Anti-Money Laundering Head Office Department and the Compliance Governance and Controls Head Office Department who will assess their capacity to actually achieve the control objectives, and if necessary, will ask for them to be enhanced.

The Business Units and other organisational units play an important part in monitoring risks of non-compliance. To that goal, they put in place all the initiatives aimed at encouraging the spread of a culture of compliance with the operators, working with them to correctly implement the training programmes defined by the Anti-Money Laundering Function in accordance with the Chief Compliance Officer Governance Area units, in association with the applicable corporate functions. Also:

- the Regional Governance Centre/Bank Control units of the Banca dei Territori Division, the CIB Controls Office of the Planning and Control Department of the Corporate and Investment Banking Division and the CLB Control Service of the Planning and Control Department-CLB are in charge of ensuring compliance of the obligations of the operational units under their responsibility, reporting any shortcomings detected and asking for any action needed to resolve them. The result of the checks made 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 units play an active role in fulfilment of requirements provided by the various regulatory frameworks and governed by specific guidelines, processes and internal procedures.

The Business Unit operational units play an active role in the fulfilment of requirements relating to anti-money laundering, combating terrorist financing and handling of embargoes. More specifically, in order to obtain greater awareness of customers, the units carry out the following activities:

- identify the customers and beneficial owners, acquiring the information and documentation (including any additional information needed in the event of relations with credit institutions and financial institutions) needed to perform the due diligence checks, and assign a risk profile to associate with the customer;
- keep the documentation acquired and keep the relative information updated;
- raise, where necessary and to the extent of their responsibility, the risk profile associated with the customers on the basis of the evidence produced by the profiling instrument;
- notify the Anti-Money Laundering Function of customers classified as high[6] risk for the related authorisation request; for medium risk customers the operational unit makes an independent decision on whether to refuse to open an account or execute an occasional transaction, involving the Anti-Money Laundering Function if considered appropriate;
- constantly monitor relations with customers and the relative transactions;
- inform the customers of the Bank's decision not to open a business relationship and/or carry out a transaction or of its intention to terminate an existing relationship.

The Manager of the operational unit (or the Relationship Manager with respect to Corporate and Investment Banking Division customers) ensures that the due diligence obligations are constantly developed in due compliance with applicable laws.

[6]With regard to non-EU correspondent entities, the documentation acquired is sent to the Operations Head Office Department for storage and data verification. With regard to high-risk customers, authorisation is the responsibility of the Anti-Money Laundering Function, in accordance with the Banca dei Territori Division or the applicable Units of the Corporate and Investment Banking Division on the basis of the type of customer. In the event of difference of opinion, the Group Control Coordination and Operational Risk Committee shall be called to make the final decision.

In order to comply with the registration obligations in the applicable computer archive, of the relationships and transactions with the customers, the operational units, where there is no procedural independence, will enter the necessary data into the computer systems, and upon request by the Anti-Money Laundering Function and/or the other control functions, will add to the missing information and/or adjust erroneous records.

Finally, the operational units carry out the following activities:

- monitor, including with the help of computer instruments, the transactions executed by customers, also considering their assigned risk profile, in order to identify anomalous transactions. These transactions, in addition to those reported by the Regional Governance Centre units in charge of controls, the CIB Controls Office of the Planning and Control Department, the Chief Audit Officer or other non-operational units, must be assessed to establish whether they involve transactions to be reported to the Head of Suspicious Activity Reporting;
- identifying breaches in regulations concerning limitations in the use of cash and bearer securities, timely communicate them to the Ministry of Economic Affairs and Finance, and sending a copy of the communication to the Anti-Money Laundering Function;
- the *ex ante* check to ensure that the payments and documents representing the related goods comply with the provisions of the Anti-Money Laundering Function with respect to operations with risky countries;
- the *ex ante* check to ensure that the payments orders by/in favour of customers do not have links with the lists known as the "*Bad Guy*" lists since they are considered to be high-risk on the basis of the profiles of the company assigned by the Group;
- checks, through the function that reports to the Manager of the line control operational unit, to ensure that the monitoring of the transactions and the assessment of the offences in terms of limitations of use of cash or bearer securities are properly developed.

4.11 Intesa Sanpaolo Group Services Units

4.11.1 Legal Affairs Head Office Department - Group General Counsel

The tasks and responsibilities of the Legal Affairs Head Office Department - Group General Counsel are described in its Organisational Code.

The Legal Affairs Head Office Department - Group General Counsel assists in monitoring the risk of money laundering, terrorist financing and breach of embargoes.
More specifically, the Finance, Insurance, Service Contracts and Special Regulations Advisory Sub-Department:

- supports the Anti-Money Laundering Function in the constant identification of applicable laws, monitoring developments, including case law developments, and providing consultation to ensure the correct and unique construction within the Group;
- shares, for the applicable legal profiles, the content of the Guidelines, the internal rules and the training courses set up by the Anti-Money Laundering Function and the other units involved, making proposals to change them and/or add to them;
- provides advice and assistance to the Anti-Money Laundering Function with regard to controversial legal aspects concerning examination of the compliance of internal processes and procedures, contracts, forms, or significant shortcomings found;
- shares, with the Anti-Money Laundering Function, standard drafts of communications to be sent to customers regarding the refusal to open an account, or suspension of an account or refusal to execute an occasional transaction.

The Criminal, Bankruptcy and Specialised Litigation Sub-Department, the Civil Litigation Sub-Department and the International Advisory and Litigation Office, each to the extent of their area of competence, manages the pre-litigation and litigation files related to breaches of embargoes.

4.11.2 Organisation Head Office Department

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

The Organisation Head Office Department is accountable for implementing organisational rules and solutions that are consistent with the objectives and guidelines of corporate policies including those established for anti-money laundering, combating terrorist financing and handling of embargoes, and has an active role in employee training processes. Within this context, the Organisation Head Office Department performs the following activities:

- supports the Anti-Money Laundering Function to provide assistance in analysing and adopting processes of organisational change and development, also ensuing from required legislative obligations concerning anti-money laundering, combating terrorist financing and handling of embargoes;
- supports and provides advice to the Anti-Money Laundering Function in the update of these Guidelines relating to anti-money laundering, combating terrorist financing and handling of embargoes, with reference to the roles and responsibilities provided for.

4.11.3 Process Management and Development

The duties and responsibilities of Process Management and Development are described in its Organisational Code.

With respect to controlling the risks of money laundering, terrorist financing and breach of embargoes, Process Management and Development carries out the following activities:

- supports the process owner to plan corporate processes and oversees the update and publication of the internal rules on anti-money laundering, combating terrorist financing and handling of embargoes;
- identifies, jointly with the Anti-Money Laundering Function and the Intesa Sanpaolo Group Services functions involved, the requirements to develop the most suitable ICT solutions to simplify the applicable processes and increase their efficiency.

4.11.4 Operations Head Office Department

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

With regard to combating the phenomena of money laundering, terrorist financing and breach of embargoes, the Operations Head Office Department carries out the following activities:

- cooperates, on the basis of the requirements set out by the Anti-Money Laundering Function, in the coordination of the requests made to the ICT Head Office Department, aimed at doing work on the ICT systems, apart from the ones most closely connected to anti-money laundering, to combating terrorist financing or to embargo handling (for example systems to manage the date stored on customer accounts, to identify anomaly indicators, for customer knowledge or for risk profiling);
- performs first level controls on the quality of data entered into the data storage archive, addressing any requests for corrective measures to be taken to the ICT Head Office Department and guaranteeing a periodic information flow to the Anti-Money Laundering Function with details of the anomalies found and the state of progress of the corrective measures implemented;
- checks, on the basis of the rules defined by the Anti-Money Laundering Function, matches with the *Sanction List* and/or the internal lists for anti-money laundering and embargo purposes (*Bad Guys*) resulting from automatic filtering systems and involving the Anti-Money Laundering Function if the suspicion is confirmed;

- checks, applying the rules defined by the Anti-Money Laundering Function, controls on payments and on bills of lading if there is a match with the Sanction List and/or the internal lists for anti-money laundering and embargo purposes (*Bad Guys*), involving the Anti-Money Laundering Function if the suspicion is confirmed.

4.11.5 ICT Head Office Department

The duties and responsibilities of the ICT Head Office Department are described in its Organisational Code.

With regard to combating the phenomena of money laundering, terrorist financing and breach of embargoes, the ICT Head Office Department is involved in the update, development and oversight of the application components, performing the following activities:

- implements and maintains, on the basis of the requirements defined by the Anti-Money Laundering Function, the ICT systems used to carry out the applicable obligations;
- controls the intactness and completeness of the flows providing input to the various application solutions used, with specific regard to the data storage archive to fulfil anti-money laundering obligations. In the event of anomalies, the ICT Head Office Department activates the necessary corrective measures and informs the Anti-Money Laundering Function;
- updates, in association with the Anti-Money Laundering Function, the *Sanction Lists*;
- makes any corrective actions reported by the Anti-Money Laundering Function and the Chief Audit Officer.

4.11.6 Cybersecurity and Business Continuity Management

The duties and responsibilities of the Cyberecurity and Business Continuity Management are described in its Organisational Code.

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

5. MACRO PROCESSES FOR COMBATING THE PHENOMENA OF MONEY LAUNDERING AND TERRORIST FINANCING

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 the guidelines and methodological rules;
- Risk Assessment and Risk Appetite Framework;
- regulatory alignment;
- consultation and clearing;
- assurance;
- spreading the culture of anti-money laundering, combating terrorist financing and embargo handling;
- interaction with the Supervisory Authorities and management of non-compliance events;
- specific requirements;
- information Flows to Corporate Bodies.

5.1 Definition of the guidelines and methodological rules

The Head of the Anti-Money Laundering Function, in accordance with the Chief Compliance Officer Governance Area Manager, 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 that risk into the Risk Appetite Framework are defined by the Head of the Anti-Money Laundering Function, in accordance with the Chief Compliance Officer Governance Area Manager and with the help of the Chief Risk Officer Governance Area Manager.

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 of the Corporate Bodies 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 Supervisory Authority Instructions with respect to anti-money laundering organisation, procedures and internal controls provide that the obliged parties assess the risk level they are exposed to in order to prepare appropriate procedures, instruments and controls (known as “self-assessment”) to be put into the Annual report.

The Head of the Anti-Money Laundering Function will make a risk assessment every year, with respect to money laundering, terrorist financing and breach of embargoes (known as AML Risk Assessment) at the level of the main Division and Group legal entities, to submit to the Company Bodies. This assessment is drawn up on the basis of the records provided by the Anti-Money Laundering Function (for the Italian Banks and Companies of the Group that apply the centralised management model) and the AML Officers of foreign Group and Branch companies (who 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-Money Laundering Function, in accordance with the Chief Compliance Officer Governance Area Manager

and with the help of the Chief Risk Officer Governance Area Manager. More specifically, the AML Risk Assessment method investigates the extent of the inherent risk and the related vulnerability through mainly quantitative indicators, integrated with qualitative assessments that correlate the type of potential risk (for example the level of customer risk) and the risk mitigation elements for money laundering, terrorist financing and breach of embargoes (for example the number of customers where the beneficial owner was registered) with respect to the size of the company.
The risk assessments at Division level result from aggregation of the relevant Company assessments 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 are 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 that aim, within the scope of defining the RAF, the Head of the Anti-Money Laundering Function, in accordance with the Chief Compliance Officer Governance Area Manager:

- 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 identified, 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 riskiness and provide for definition of specific management guidelines, monitor operations and take 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 assessments also contribute to the Integrated Risk Assessment - prepared within the scope of the Group Control Coordination and Operational Risk Committee, Integrated SCI session - aimed at providing a summarised viewpoint of the assessments produced by each Group Control Function as a whole, and the main legal entities and Business Units, in accordance with the methods in use with each Function.

5.3 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;
- the assessment of the impact of the applicable laws on the company processes and procedures, and the consequent proposal for organisational and procedural amendments aimed at ensuring adequate control of the risks.

The Anti-Money Laundering Function is in charge of continued identification of 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 the applicable laws and consequent proposal of guidelines, rules, processes and procedures is managed by the Anti-Money Laundering Function, with assistance from the Organisation Head Office Department and Process Management and Development, and for the legal aspects, the Legal Affairs Head Office Department - Group General Counsel.

Alignment with the regulations is aimed at the *ex-ante* definition of a framework that substantially complies with the law, in accordance with the following indicators:

- the guidelines and main strategies to manage the areas with crossover impacts on Group operations are defined in specific guidelines that have to be approved by the Corporate Bodies;
- the rules governing the relevant areas are set out in rules documents that illustrate the methodological aspects, operational mechanisms, rules of behaviour and the restrictions involved, also in implementation of the guidelines, and in compliance with the policies contained therein;
- the processes, where standardised, are supported by ICT procedures and instruments that can assist and guide the behaviour of the staff, in order to ensure they behave honestly;
- in the more sensitive processes, the guidelines and rules provide for prior involvement by the Anti-Money Laundering Function;
- the processes provide for a control system that can monitor, over time, the effectiveness of the controls, also taking account of changes in the laws and in business.

5.4 Consultation and clearing

Risk is controlled on a preventive basis, including through:

- the consultation and assistance given to the Corporate Bodies and the Bank units on the interpretation and application of external and internal rules;
- the prior assessment of compliance with prevailing laws (*clearing*) on:
  - innovative projects, including starting up new activities and entering new markets;
  - new products and services to be marketed and/or significant changes to existing ones;
  - sensitive cases and transactions in relation to which the company processes, as governed by the Guidelines and the Rules, provide for the prior assessment by the Anti-Money Laundering Function.

The Anti-Money Laundering Function provides consultation and assistance to the Company Bodies and the other company units on matters relating to the actual application of external laws to the company processes and activities, and the behaviour to adopt.

With regard to the clearing activities, the Anti-Money Laundering Function 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 assessments of the Anti-Money Laundering Function are made by adopting formats that are pre-established to the greatest extent possible, and that must contain at least the following elements:

- subject of appraisal;
- external and/or internal applicable regulatory framework;
- elements that are relevant to the case being analysed, and significant for the purpose of the assessments;
- summarised considerations showing the level of consistency with the letter and spirit of the external and internal laws, any residual risks and the recommendations made.

The depth of the analyses made is proportional to the level of complexity and novelty of the cases considered and the applicable law.

5.5 Assurance

5.5.1 The assurance model

The control over the risk entails, also on a preventive basis, 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 units.

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 and business units, 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 taking them back to areas of operational and management uniformity;
- the monitoring of the correct application of the applicable methodological and control framework by the operational and business units to the second level control functions, by checking both the design of the processes, procedures and controls and correctly applying the applicable controls.

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

- when defining or reviewing the company processes, also following developments in the external regulatory framework, the Anti-Money Laundering Function will set the control objectives, informing the operational and business units, and the applicable organisational units;
- the operational and business units, in association with the Anti-Money Laundering Function, the Compliance Governance and Controls Head Office Department, the Organisation Head Office Department and Process Management and Development, to the extent of their responsibilities, will define the first level controls that are considered suitable for actually achieving the control objectives, and then carry them out. The first level controls identified by the Business Units and other operational and business units are submitted for inspection by the Anti-Money Laundering Function and the Compliance Governance and Controls Head Office Department who will assess their capacity to actually achieve the control objectives, and if necessary, ask for them to be enhanced;
- the Anti-Money Laundering Function 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; they may be performance type controls on a remote basis of the phenomena monitored, controls also "on site", of the processes carried out by the operational units and their efficiency, controls on the correct execution of the first level controls by the operational units; in accordance with the level of risk found, and taking account of capacity restrictions, the frequency of the controls may be continuous or periodic, on an inter-annual, annual, or multi-annual basis, or on a once-off basis.

5.5.2 How the activities are carried out

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 one-off 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-Money Laundering Function, on an annual basis, taking account of the results of the 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 operational and business units; the report, to be carried out using, where possible, the pre-defined formats, must contain the following elements:

- characteristics of the action (objective of the control, applicable internal/external regulatory framework);
- details of the checks carried out and relative results;
- summarised considerations showing the residual risks and the suggested mitigation actions.

The individual organisational units are responsible for the planning and implementation of the corrective actions; the above-mentioned Head Office Departments monitor and track the state of progress of the actions identified.

5.5.3 Interactions with the other control Functions and information flows

In carrying out the checks, the Anti-Money Laundering Function and the Compliance Governance and Controls Head Office Department also use the results of the 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.

The collaboration methods between the Corporate Control Functions and the relative information flows are set out in the Integrated Internal Control System Regulation.

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, that the first, second and third level control Functions take part in to:

- get more in-depth information on the findings from the control activities, encouraging the standard, 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, integrated basis.

The Anti-Money Laundering Function 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 aim:

- they receive and send the information flows reported in the Integrated Internal Control System Regulation;
- the other company units must inform them, in a timely, 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 Spreading the culture of anti-money laundering, combating terrorist financing and embargoes;

The dissemination, 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.

Efficient application of regulations relating to anti-money laundering, combating terrorist financing and handling of embargoes must incorporate full awareness of the aims and principles underlying the system.

The Anti-Money Laundering Function 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 the training requirements relating to the applicable matters and preparing the content of the training initiatives for all the Bank resources, in order to ensure that the staff, with specific attention to the sales force for the products and the managers of the business units, have adequate awareness of the applicable laws, the obligations and related responsibilities, the consequences resulting from the failure to fulfil said obligations and to ensure they are able to knowingly use support instruments and procedures in fulfilment of the requirements established by the law.

The Anti-Money Laundering Function, with the assistance of the Development Policies and Learning Academy Head Office Department and the People Management & HR Transformation Head Office Department monitor development of the training programmes, checking 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 the traditional training activities, the Anti-Money Laundering Function, under the protection of the Group Control Coordination and Operational Risk Committee, and in association with the Development Policies and Learning Academy Head Office Department, organises and takes part in the specific initiatives aimed at spreading the culture of risk and expanding the level of awareness of the approach to risk requested, including in particular:

- *induction sessions* for the Corporate Bodies and workshops for top management on especially delicate or timely matters;
- actions to make the business units more aware of the specific risks aspects involved in ordinary operations;
- diagnostic activities in order to understand the level of dissemination of the risk culture at all company levels, in terms of consistency of the perceptions and behaviour with respect to the required guidelines and policies.

Specific training programmes are also provided to staff in the Anti-Money Laundering Function so that they are always updated on risk developments in the area.

5.7 Interaction with the Supervisory Authorities and management of non-compliance events

Relations with the Supervisory Authorities and management of non-compliance events are occasions of special relevance when controlling risk. The Anti-Money Laundering Function provides for management of the following in the areas it is responsible for:

- relations with the Supervisory Authorities, coordinating the activities needed to provide feedback to the Authorities;
- non-compliance events, providing assistance and cooperation to the unit in order to ensure the identification and implementation of the actions to undertake to fill any organisational and/or procedural gaps.

The interaction processes also include sending specific reports to the Supervisory Authorities, in accordance with the requirements defined by the law with respect to anti-money laundering, combating terrorism and handling embargoes. This reporting includes:

- transmitting on a monthly basis, to the Financial Intelligence Unit (FIU), the aggregate date concerning the records in the storage archive;
- transmitting the reports of suspicious activity to the Financial Intelligence Unit (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 that will be issued by the Financial Intelligence Unit (FIU).

5.8 Specific requirements

5.8.1 Customer awareness and profiling

The following is provided for in order to guarantee customer due diligence:

- the identification of customers and beneficial owners, the acquisition of 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. If it is not possible to comply with customer due diligence obligations, an ongoing relationship cannot be initiated or a transaction cannot be carried out (or the assessment of what procedures to adopt to interrupt the existing relationship);
- customer profiling on the basis of the risk of money laundering, terrorist financing and breach of embargoes, subject to standardising the process at Group level;
- authorisation to open a new relationship, execute an occasional transaction or maintain an existing relationship on the basis of the risk profile assigned to the customer. For customers classified as high risk, authorisation must be provided by the Anti-Money Laundering Function; authorisation is provided directly by the operational units for medium risk customers, which may involve the Anti-Money Laundering Function, whenever considered appropriate;
- constant monitoring of the business relationships, by the operational units, in order to keep awareness of the customer up to date, and ensure the consistency of the operations with the scope of the relationship declared by the customer; this is to intercept any “unexpected”, anomalous or inconsistent transactions with respect to the economic and financial profile of the customer or any news of significant events the relate to the customer;
- the periodic update of the information on the knowledge of the customer and the periodic review of the risk profile;
- authorisation to go ahead or not, issued by the Anti-Money Laundering Function, for customers, who, during collection of information or update of the register, are found to be on the Sanction Lists, also following checks carried out by the applicable functions of the Operations Head Office Department.

5.8.2 Data retention

In order to record the customer identification data and the data relating to the relationships begun and the transactions carried out, data is input into the data storage archive to comply with anti-money laundering obligations and process the data; this archive is managed by the Anti-Money Laundering Function and by the ICT Head Office Department, each to the extent of their responsibility, in order to ensure the clarity and completeness of the information, that it is stored and easy to consult. The aggregate data concerning the operations of the Bank to send, on a monthly basis to the Financial Intelligence Unit (FIU), by the Anti-Money Laundering Function, is also determined on the basis of this archive.

5.8.3 Monitoring transactions

The main processes to guarantee control of the transactions carried out by customers are as follows:

- *ex ante* monitoring, by the operational units who 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 securities. The operational units may also use the support of the consultation units that report to the Head of Suspicious Activity reporting to decide whether to carry out a transaction or not, and ask the Financial Intelligence Unit (FIU) for a suspension order in cases of clear risk;
- *ex ante* control of the payments and documents representing goods by checking them against the *Sanction Lists* and/or the internal Group lists *(Bad Guys)*, and checking the findings from the control procedures. These checks firstly involve the Operations Head Office Department and the *operational units* that perform the transactions, which, if necessary, require authorisation from the Anti-Money Laundering Function to go ahead with the transactions;
- *ex post* monitoring of the transactions by the operational units in order to identify anomalous transactions, including with the assistance of the automatic anomaly indicator 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*[7] *in United States currency* and (ii) operates with payable-through accounts[8] only on condition that customer due diligence is guaranteed by the counterparty bank using said payable-through accounts[9].

5.8.4 Reporting suspicious activity

In order to ensure fulfilment of the obligations on reporting the transactions considered suspicious, the reporting procedure, in accordance with the regulatory requirements is set out into two stages:

- first level reporting by the Managers of the company operational units, 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-Money Laundering Function 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 units fall under the above-mentioned examination.

5.9 Information Flows to Corporate Bodies

The communication processes with respect to the Corporate Bodies provide for the following:

---

[7]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.

[8]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' behalf.

[9]Specifically, Legislative Decree no. 231/2007 provides that in the case of a correspondent account held with a non-EU credit institution the Bank must ensure that it has verified the identity of the customers who have direct access to the payable-through accounts, has constantly fulfilled the customer due diligence obligations and, when requested, can provide the data acquired in fulfilling said obligations.

- 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; communication to the Supervisory Authorities or the Ministry of Economic Affairs and Finance is only sent subsequently;
- half-yearly report on inspection activities performed, actions taken, shortcomings found and corrective measures to be taken as well as on personnel training activity;
- half-yearly report on training activities on anti-money laundering, combating terrorist financing and handling of embargoes;
- specific disclosures on particularly significant matters.

6. GROUP GOVERNANCE

6.1 General principles

Considering its territorial base, the Group systematically adopts a unified approach to anti-money laundering, combating terrorist financing and handling of embargoes, with guidelines, rules, processes, and ICT controls and instruments that are reasonably standard at Group level. To that end, the Group Companies have to implement these Guidelines, adjusting them to their own corporate context, and in the case of foreign Companies, to the specific nature of local laws, submitting them for approval to the Supervisory Body.

The strategic decisions taken at Group level concerning management of the risk 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 the situations of their companies. To that end, 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 scope of the Intesa Sanpaolo Group, the specific tasks attributed to the Anti-Money Laundering Function are carried out on the basis of two separate models which take account of the Group's operational and territorial organisation. More specifically, it provides for the following:

- for specifically identified Italian Banks and Companies whose operations are highly integrated with the Parent Company, the centralisation of the risk monitoring activities relating to money laundering, terrorist financing and breach of embargoes with the Parent Company Anti-Money Laundering Function (centralised management model). The choice to centralise the activities is backed by assessment and documentation, using Group logic, of the risks, costs and benefits associated with it; this analysis is periodically 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 and a Manager to report suspicious activity who are given the responsibility for these matters (the steering, coordination and control model).

Italian Companies that have not been asked to establish the Anti-Money Laundering Function monitor risk within the scope of the Organisation, Management and Control Model pursuant to Legislative Decree no. 231/2001, using, for any specific matters, support by the Group Anti-Money Laundering Function.

In execution of the role providing steering, coordination and control to the Group Companies, the Parent Company Anti-Money Laundering Function and the Compliance Governance Control Head Office Department operate in association with the Business Units, putting adequate exchanges of information into place and maximising their potential synergy. The International Subsidiary Banks Division in particular, works with the Compliance Governance Controls 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 handling of embargoes, also taking account of the specific corporate context and the local regulations that apply.

6.2 The centralised management model

In the Banks and 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-Money Laundering 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 applicable contracts.

The centralised management model requires the appointment of a local Anti-Money Laundering Representative (AML Representative), who, working in close coordination with the Parent Company, oversees the processes linked to anti-money laundering, terrorism combating and embargo handling regulations in each individual Company. The appointment and discharge of local AML Representatives is subject to the binding opinion of the Group Head of Anti-Money Laundering.

The local AML Representative:

- monitors the procedures for fulfilling obligations concerning the combating of money laundering, terrorist financing and breach of embargoes and monitors the level of service provided by the Parent Company's functions that are responsible for the centralised activities;
- draws the attention of the Corporate Bodies, the Group Head of Anti-Money Laundering and the applicable units to any anomalies in the services provided and suggests improvements;
- monitors, on a monthly basis, the representation drawn up by the Compliance Governance and Controls Head Office Department of the monitoring indicators taken from the monitoring system and defined in accordance with the Anti-Money Laundering Function. In addition to the information concerning each Bank, the document in question shows, on a comparative basis, the situations subject to constant checking by the Anti-Money Laundering Function that the AML Representative has to investigate more closely, if necessary with the support of the first and second level Control functions, and shows the information to the Control Bodies, focusing attention on the data related to the applicable Bank;
- informs, in a complete and timely manner, the Group Head of Anti-Money Laundering, of the aspects of specific interest regarding the results of the control activities carried out and any significant events.

With regard to the coordination with the Parent Company, the AML Representative provides local monitoring services for the Parent Company Anti-Money Laundering Function. This monitoring is carried out by:

- timely reporting with respect to the Anti-Money Laundering Head Office Department units of any significant events that emerge at the applicable Bank;
- constant cooperation with the central and local control units;
- specific analyses or controls that may be requested by the Anti-Money Laundering Function with respect to cases, found by the central offices, that require timely, focused action *in situ*.

The centralised management model both defines the guiding principles and standards of conduct that the Companies must adopt in managing the main obligations concerning the combating of money laundering, terrorist financing and breach of embargoes, and provides that the Parent Company's Anti-Money Laundering Function:

- identifies and updates, in accordance with the Compliance Governance and Controls Head Office Department, the first and second level control system aimed at preventing and combating the risk of money laundering, terrorist financing and breach of embargoes;
- defines, in accordance with the Compliance Governance and Controls Head Office Department, any corrective actions on the first and second level control system and the control objectives, in accordance with the applicable company functions of the Group Company and Parent Company, taking into account the developments in the applicable context and the results of the control activities, and coordinating the various functions involved in the implementation stages;

- assesses the customers that, during registration or update of the data register, are found to have a match on the Sanction Lists, if the investigation by the applicable Group Companies or Parent Company do not provide for independent decisions;
- supervises the data storage archive to fulfil the anti-money laundering obligations and manages it with the help of the ICT Head Office Department; a single service centre is established at the Parent Company pursuant to Legislative Decree no. 231/2007 for that purpose;
- defines the instrument requirements for the due diligence and customer profiling support tools;
- carries out, following investigations by the applicable corporate functions of the Group Company and the Parent Company, the assessment of the transactions and/or customers where matches were found on the Sanction Lists/were blocked/reported by the payment reporting system; if there is a definitive decision to block the operations or the funds, the Group Anti-Money Laundering Function makes the relative notification to the Financial Intelligence Unit (FIU);
- prepares, with the assistance of the AML Representative, and certifies the standard questionnaire referring to the adequacy of the company with respect to anti-money laundering, combating terrorist financing and embargo handling requirements required by the foreign Correspondents;
- prepares periodic summary reports or specific reports in the event of particularly serious events, to send to the Corporate Bodies and Senior Management.

With reference to potentially suspicious activities, the Group operational units promptly report, on a first level basis, to the Group Delegate, who is assigned, by the legal representative of each Company, the authority to report suspicious activity to the Financial Intelligence Unit (FIU). Furthermore, the Company Control Bodies notify the Group Delegate of any offences pursuant to article 46, paragraph 1, letter a) of Legislative Decree no. 231/2007, revealed during the exercise of its functions. The Group Delegate acquires, directly or through the Group Companies, information on the scope, including information in the data storage archive, to fulfil the anti-money laundering obligations.

With respect to the offences pursuant to article 46, paragraph 1, letter b) and article 51, paragraph 1, the control units of the Group Companies promptly establish and report said offences to the Parent Company's Anti-Money Laundering Function, which, through the Function Head, and on the basis of the evidence resulting from the second level control activity, informs the Companies' Control Bodies so they can send the relative communication to the Supervisory Authorities or the Ministry of Economic Affairs and Finance; the communication by the aforesaid Bodies must also be made if they discover offences in the performance of their duties.

6.3 The steering, coordination and control model

The Group companies and the foreign branches to whom the steering, coordination and control model applies, set up their own Anti-Money Laundering Functions and appoint the relative Head (who normally also fulfils the role of Head of Suspicious Activity Reporting), in the Italian Companies on the basis of the delegation of authority assigned, pursuant to Legislative Decree no. 231/2007, by the Company's legal representative, and in the foreign Companies and branches, on the basis of the requirements under local regulations.

The steering, coordination and control model activities are carried out by the following for said Entities:

- Anti-Money Laundering Head Office Department with reference to the Foreign Branches of Intesa Sanpaolo and the other Banks and Companies subject to centralised management;
- Compliance Governance and Controls Head Office Department with reference to the other Italian and foreign Group companies to which the steering, coordination and control model apply.

The appointment, discharge and actions of the merit-based recognition of the Head of the Anti-Money Laundering Function at the Group Companies and Foreign Branches are submitted for the

prior, binding opinion of the Group Head of Anti-Money Laundering, subject to agreement with the Compliance Governance and Controls Head Office Department for the Group Companies.

The Head of the Anti-Money Laundering Function at Group Companies and Foreign Branches:

- functionally reports to the Group Head of Anti-Money Laundering for implementation of the choices made by the Parent Company with regard to risk-management policies, processes and procedures with respect to money laundering, terrorist financing and breach of embargoes; for the Group Companies, reporting is carried out in accordance with the Compliance Governance and Controls Head Office Department;
- informs, in the case of Group companies, the Compliance Governance and Controls Head Office Department, and in the case of foreign Branches, the Anti-Money Laundering Function, on a complete and timely basis, of the results of the controls carried out on the basis of macro control objectives provided by the Head of the Group Anti-Money Laundering Function, and of any significant events. In this regard, it also provides half-yearly reports on issues governed by the guidelines set forth by the Parent Company[10];
- liaises with the Supervisory Authorities to stay up to date on the legislative framework and operate in compliance with regulations in force regarding the business model adopted and/or the host country, coordinating, in the case of Group Companies, with the Compliance Governance and Controls Head Office Department, and in the case of foreign Branches, with the Anti-Money Laundering Function, to guarantee compatibility with these Guidelines and facilitate dialogue with the Supervisory Authorities. These Functions assist 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, in the case of Group companies, through the Compliance Governance and Controls Head Office Department, the Anti-Money Laundering Head Office Department, if local laws do not permit application of measures for anti-money laundering, combating terrorist financing or handling of embargoes that are equivalent to those of the European Community, so that the Group Head of Anti-Money Laundering can inform the Bank of Italy, pursuant to Legislative Decree no. 231/2007.

The Head of Suspicious Activity Reporting of Group Companies and Foreign Branches to whom the steering, coordination and control model applies, sends the Group Delegate a copy of the reports sent to the Financial Intelligence Unit (FIU) or the applicable foreign Unit[11], in addition to the filed ones, along with the reason that led to the filing, without prejudice to local rules governing banking and/or professional secrecy, or other local regulations (on AML matters) that would prevent the sending of reports pertaining to the relative foreign Companies of the Group to the Group Delegate. They are sent using procedures designed to guarantee maximum confidentiality of the identity of the first level Manager making the report. In order to investigate anomalous transactions or relationships at Group level, the Group Delegate may use all units in the Group Companies, also if the steering, coordination and control model is applied to said Companies.

The Head of the Anti-Money Laundering Function of Group Companies and Foreign Branches is entrusted with responsibility for authorising the execution of an occasional transaction or the opening and maintaining of existing relationships with high risk customers and for assessing customers who, during the registration or the update of their personal details, are found to be included in the Sanctions Lists.

---

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

[11] Article 33, paragraph 2 of EU Directive 849 of 2015 provides that reports are to be sent to the Financial Intelligence Unit (FIU) of the member state in the territory where the obliged party sending the information is located.

The Anti-Money Laundering Head Office Department and Compliance Governance and Controls Head Office Department, each to the extent of its responsibility, define the Group policies and oversee their proper application by the Companies and the foreign Branches in steering, coordination and control in accordance with the model defined in the Intesa Sanpaolo Group Compliance Guidelines. More specifically, said Departments disseminate the general standards or at least the minimum standards of behaviour to follow with respect to:

- risk assessment (methods and relative instruments and the data on which the inherent risk assessment and relative controls are based);
- macro-objectives to provide for with regard to the control system for preventing and combating the risk of money laundering, terrorist financing and breach of embargoes;
- due diligence obligations (information set and methods to carry out due diligence on the customer, reviewing their risk profiles and criteria for customer acceptance and abstention obligations); the foreign Companies and Branches have to operate, where the customers are shared with other Group entities, on the basis of the highest risk profile among those assigned by said entities (known as the “harmonisation criteria”);
- registration and data storage obligations (procedures for registration, storage and management of information and documentation acquired from customers);
- reporting obligations (procedures to assess potentially suspicious activity in order to make any first level reports, timeliness of reports, traceability of the assessment procedure and clear identification of responsibilities); enhanced due diligence obligations for transactions (processes and procedures to be adopted when monitoring transactions performed by customers including the control of customer’s operating activity and checking against the Sanction Lists);
- limitations in the use of cash and bearer securities (processes and procedures for obligations relating to limitations in the use of cash and bearer securities);
- transaction filtering (processes and procedures relating to the control of international operating activity in compliance with regulations on embargoes including transaction filtering, checking counterparties and other elements included in the Sanction Lists);
- staff training (minimum contents for guaranteeing adequate training levels such as the type of courses and the users they are designed for);
- control system (types and methods adopted to carry out the controls to be performed to check compliance with established obligations);
- requirements for secondary application solutions.

In order to carry out its duties, the Anti-Money Laundering Head Office Department and the Compliance Governance and Controls Head Office Department have access, with respect to the foreign Branches and Group Companies, to all the activities and any relevant information with regard to compliance, including through direct interaction with the staff.

The International Subsidiary Banks Division and the Corporate and Investment Banking Division, for their areas of competence, support the Foreign Companies and Foreign Branches in order to guarantee alignment between the objectives relating to anti-money laundering, combating terrorist financing and handling of embargoes, and the business objectives, and work to solve any weaknesses and facilitate and promote proactive management of the applicable obligations.

The Parent Company’s Chief Audit Officer steers and coordinates the activity of the auditing units in the Group Companies and foreign branches to ensure standardised controls and adequate attention to the various types of risk, including the risk of failure to comply with legislative provisions for preventing and combating money laundering, terrorist financing or handling of embargoes.