VÚB BANKA

VÚB Group AML Guidelines

FOR THE FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING AND THE HANDLING OF THE EMBARGOES

VÚB, a.s.
Date: July 1, 2020

CONTENTS

1 KEY TERMS DEFINITION / INTRODUCTION

Expression	Acronym	Interpretation
1.AML		Anti Money Laundering means protecting the bank from legalizing the proceeds of crime (anti-money laundering and terrorist financing)
2.VUB Bank		Všeobecná úverová banka, a.s.
3.FIU		Financial Intelligence Unit

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

The Guidelines in this document identify the applicable standards and define the risk management model regarding money laundering, terrorist financing and breach of embargoes of Intesa Sanpaolo, setting out:

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

The Guidelines are reviewed on an annual basis and any amendments are subject to the approval of the Management Board and to the acknowledgement of the Audit Committee and Supervisory Board.

The Guidelines are set out in valid operational terms in the Rules for Managing Compliance Macro-Processes (valid internal policy of VUB Bank no. 913 - Compliance Rulebook), in the valid internal policy of VUB Bank no. 742 (VÚB Bank aml rulebook on measures and actions for anti-money laundering and counter-terrorism financing), in the valid internal working procedure of VUB Bank no. 660 (AML program (process „know your customer“)) and of VUB Prague (no. 905 System of Internal Principles, Procedures and Control on Measures and Actions for Anti-Money Laundering and Counter-Terrorism financing), which define specific, individual obligations. The Compliance Rulebook is reviewed annually, in keeping with organisational and operational changes to the risk management model for money laundering, terrorist financing and the breach of embargoes and amendment must be approved by the Bank Compliance Officer and AML Officer and by the competent structures of the VUB, as well as submitted to the attention of the Audit Committee of the Bank.

2 OBJECTIVES, DEFINITIONS AND PRINCIPLES

2.1 Objectives

- This Document aims at:
- setting out the main roles and responsibilities of the Bank’s Corporate Bodies and organizational units which participate in prevention of money laundering, fight against terrorism financing and dealing with embargoes;
- defining principles applied by the Bank in the process prevention of money laundering, fight against terrorism financing and dealing with embargoes.

2.2 Definitions

"Money laundering" means:

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

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

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

3 LEGAL FRAMEWORK

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

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

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

Main European Union law is as follows:

- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 (the “IV Directive”) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30/05/2018 ("V Directive"), amending Directive EU 2015/849;
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;
- Commission Delegated Regulation (EU) 2016/1675, as amended, supplementing the IV Directive by identifying high-risk third Countries with strategic deficiencies;

- Commission Delegated Regulation (EU) 2019/758 supplementing the IV Directive with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third Countries (outside the European Economic Area, the "non-EEA Countries"); and, specifically, on money laundering and terrorist financing:
- Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism;
- Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban.

Basic measures and activities aimed at preventing and detecting money laundering and terrorism financing have been stipulated by the following Slovak legislation:

- Methodological Guideline No 3/2019 of the Financial Market Supervision Unit of National Bank of Slovakia of 29 April 2019 regarding the prevention by banks and foreign bank branches of money laundering and terrorist financing;
- Act 297/2008 of 2 July 2008 on the Prevention of Legalization of Proceeds of Criminal Activity and Terrorist Financing and on Amendments and Supplements to Certain Acts as amended (further also "AML Act");

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

As the Intesa Sanpaolo Group operates in the United States it has signed the "US Patriot Act Certification" and is required to observe US law in its business and financial transactions carried out in the United States, such as payment orders in dollars, and in general, in transactions carried out on its own behalf and on behalf of third parties. The transactions that the Bank undertakes on its own account and/or on behalf of its customers are also subject to United States laws when these transactions involve a relationship with parties subject to US legislation (for example US banks, foreign branches of US banks and US Subjects in general).
VUB Bank - at the moment of the publication of these Guidelines – is not operating in the U.S.A.

The common principles of the applicable legal framework are:
- the obligation to carry out customer due diligence, obtaining suitable information to identify the customer, the beneficial owner and the purpose of the account or transaction;
- the obligation to retain data for anti-money laundering obligations;

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

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

The organisation required by law must be based on:
- the establishment of a specific function to prevent and combat money laundering and terrorist financing transactions, the appointment of a person in charge and of an officer to report suspected money laundering/terrorist financing;
- a clear definition of roles, duties and responsibilities, and procedures that guarantee compliance with customer due diligence and suspicious activity reporting obligations, as well as obligations to store documentation and records of the accounts and transactions and suspicious activity reporting;
- a system of control functions that is coordinated, also through suitable information flows and is adequate for the size of the company and its complexity, and for the type of services and products offered as well as the extent of risk that may be associated with the characteristics of customers;
- a strong emphasis on the accountability of employees and external staff and controls that are suitable for monitoring their compliance with regulatory obligations and internal processes as well as their adoption.

The regulation requires effective coordination of controls for the prevention and combating of money laundering and terrorist financing at a Group level, and the procedures adopted by VUB Group to be in line with Group standards and ensure that information is shared at consolidated level. In the case of non-EEA Countries[1] which have limits on the circulation of information, specific corrective measures shall be adopted, in line with the provisions of the aforementioned Commission Delegated Regulation (EU) 2019/758.

3.2 The legal framework concerning embargoes

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

[1] The European Economic Area, abbreviated as EEA, consists of the Member States of the European Union (EU) and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway; excluding Switzerland). The United Kingdom formally left the European Union (EU) on 31 January 2020 and became a third country. A transition period began on 1 February 2020 and is due to end on 31 December 2020. In particular, EEA include: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

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

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

Applicable legislation on the management of embargoes may be classified as follows:
- European legal instruments;
- primary and secondary Slovak legislation.

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

In addition to the provisions of directly applicable Regulations, at national level the main legislative framework consists of:
- Act No. 39/2011 Coll. on Dual-Use Items and on Amendment to Act of the National Council of the Slovak Republic No. 145/1995 Coll. on Administrative Fees as amended
- Act No. 289/2016 Coll. of 11 October 2016 on the execution of international sanctions

As the Intesa Sanpaolo Group operates in the United States, US legislation, comprising the "US Patriot Act" mentioned above, as well as regulations on economic and commercial sanctions adopted by the US Government, mainly through the Office of Foreign Asset Control (OFAC) of the Treasury Department, as part of foreign and national security policies, are of particular importance[2].

The applicable legal framework, which has obvious connections with legislation on money laundering and terrorist financing, mentioned above, establishes restrictive measures and sanctions against governments of third Countries, non-government organisations, and natural or legal persons in relation to:
- arms embargoes;
- other specific or general commercial restrictions (ban on export and import);
- financial restrictions (freezing of assets and resources, bans concerning financial transactions, restrictions on export credits or investments);
- criminal sanctions for entities financing terrorist or subversive associations and exporting dual-use products in breach of regulations governing dual-use.

The legal framework requires the Bank to adopt measures guaranteeing:
- controls of records and customer transactions, regarding imports and/or exports;
- the traceability of controls on transactions originating from/for Countries, persons and entities against whom restrictions have been established;
- the freezing of goods and resources attributable to designated parties that the restrictive measures apply to, and forwarding the resulting communications to the Financial Intelligence Unit (FIU);

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

- the reporting of transactions suspected to finance terrorism or activities for the proliferation of weapons of mass destruction.

4 GENERAL PRINCIPLES OF THE GOVERNANCE MODEL

These Guidelines fall within the scope of the structure defined by the Group through the valid 807 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 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, monitors the efficient implementation, function, compliance and update of the relative Model and its ability to prevent and combat the commission of the crimes;
- the Anti-Money Laundering Function continuously checks corporate processes and procedures, and proposes, in association with the applicable corporate functions, the organisational and procedural changes required and/or advisable to ensure adequate control over the risk of money laundering, terrorist financing and breach of embargoes;
- other second level Corporate Control Functions and the support Functions work with the AML Department so that it can develop its own risk management procedures that are consistent with corporate strategies and operations;
- the operational, business and support functions follow the corporate processes and procedures, verifying their implementation through appropriate level I controls, with a view to full and complete compliance with applicable laws and standards of conduct;
- the Head of the Internal Audit and Control Department, within the scope of his/her ordinary activities, monitors the degree of adequacy of the corporate organisational structure and its compliance with applicable laws on an ongoing basis, and also oversees the functioning of the entire internal control system.

In monitoring risks relating to money laundering, terrorist financing and breach of embargoes, the VUB Group[3] has adopted the following general standards:

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

[3] VUB subsidiary VUB Leasing and foreign organizational unit of VUB – VUB Prague branch

5 ROLES AND RESPONSIBILITIES

Responsibility for prevention of activities relating to the legalization of income derived from criminal activity and AML tasks performance, including the protection against terrorism financing, shall be within the authority of the Management Board, acting through a separate internal department (AML Department).

The oversight of the processes for the fight against money laundering and terrorism financing and managing embargoes demands involvement of the following Bank's interacting bodies and organizational units with their different roles and responsibilities:

- *SUPERVISORY BOARD*
- *MANAGEMENT BOARD*
- *AUDIT COMMITTEE*
- *COMPLIANCE DEPARTMENT*
- *ANTI - MONEY LAUNDERING DEPARTMENT*
- *AML OFFICER*
- *LEGAL DEPARTMENT*
- *OPERATIONS AND IT DIVISION*
- *RISK MANAGEMENT DIVISION*
- *HUMAN RESOURCES AND ORGANIZATION DEPARTMENT*
- *RETAIL AND CORPORATE BANKING DIVISIONS*
- *INTERNAL AUDIT AND CONTROL DEPARTMENT*
- *INFORMATION SECURITY AND BUSINESS CONTINUITY MANAGEMENT OFFICIES*

5.1 Supervisory Board

The Supervisory Board carries out the following activities:

- acknowledges, on a proposal from the Management Board, the VUB Group AML Guidelines and AML Rulebook and related updates;
- monitors the compliance with anti-money laundering and counter terrorism financing provisions;
- supervises the implementation of AML regulations; the Supervisory Board may establish committees such as Audit Committee which have a right to review/investigate all matters of the Bank;
- provides its opinion to the Management Board relating to the appointment of the AML Officer and his/her Deputy;
- approves the reports submitted by the AML Officer (annual report, risk assessment, semi-annual and ad-hoc reports).

5.2 Management Board

The Management Board is responsible for establishing and functioning of an Anti-Money Laundering Department (hereinafter referred to as the "AML"). The Management Board carries out the following activities:

- defines the VUB Group AML Guidelines and AML Rulebook, and related updates, on a proposal from AML Officer, which submits to the acknowledgement of the Supervisory Board;
- appoints/removes the AML Officer, and his/her deputy, taken into consideration the opinion of the Supervisory Board, with the prior binding opinion of the Head of Anti Financial Crime (AFC) Head Office Department;
- approves the training programme concerning anti-money laundering;
- defines the information flows intended to ensure to the governing bodies and the control functions full awareness and management of the requirements;
- requires the AML Officer to report on AML activities semi-annually;
- evaluates the adequacy and effectiveness of AML risk management and control system;
- reviews the violations of AML provisions promptly communicated by the Audit Committee;
- sets up and updates the internal procedures, detailing operational processes implemented to manage the AML requirements and the roles and responsibilities attributed to involved structures;
- assesses the organisational structure and the adequacy of the internal control system with regard to pertinent obligations, submitting them to review if necessary;
- evaluates and ensures the main remediation actions carried out in relation to relevant violations of AML provisions;
- rules on strategic decisions concerning anti-money laundering and counter terrorist financing, which submits to the acknowledgement of the Supervisory Board.

5.3 Audit Committee

The Audit Committee carries out the following activities:
- acknowledges, on a proposal from the Management Board, the VUB Group AML Guidelines and AML Rulebook and related updates;
- verifies the compliance with anti-money laundering and counter terrorism financing provisions, assessing the effectiveness and efficiency of the governance model, also based on the examination of the results of periodic control activities concerning AML conducted by Internal Audit and Control Division and AML Department;
- addresses the evaluation of detected anomalies ensuring the implementation of the necessary remediation actions;
- evaluates any violations of the AML provisions (customer due diligence, record keeping, etc.) based on the information flows received from the other Corporate Bodies and from the AML Officer;
- requires the AML Officer to regularly report on AML activities.

5.4 AML Department

The duties and responsibilities of the AML Department are described in its Organizational Code and in the valid internal procedure No. 807 Integrated Internal Control System Regulation.
The AML Department, in a capacity as Anti-Money Laundering Function:
- is independent from the operational entities and has enough resources to carry out its duties from a qualitative and quantitative standpoint;
- reports directly to Senior Management;
- has access to all business activities, as well as significant information for carrying out its duties.

The AML Department monitors risks of money laundering, terrorist financing and breach of embargoes, carrying out the following activities:
- defining the guidelines, methodological and processes to adopt for risk management;

- checking the compliance of the Bank with local AML Regulatory References and manages the relations with local supervisory authorities;
- monitoring the risk assessment process, contributing to its integration in the Risk Appetite Framework (RAF) of the Bank and planning management actions;
- monitoring the regulatory alignment process, guaranteeing that external regulations are monitored at all times and adequately translated into guidelines, rules, processes and internal procedures;
- advising and assisting Corporate bodies and other Bank entities on interpreting and adopting internal and external regulations, and assessing conformity to applicable regulations in advance (clearing) for innovative projects, including the start of new activities and entry on new markets, new products and services to market and sensitive transactions;
- establishing the control objectives to mitigate risk, cooperating with other company entities in defining first and second level controls, and reviewing the results to define and monitor mitigation actions;
- assisting in disseminating an adequate risk culture at all levels of the company;
- managing relations with the Supervisory Authorities and nonconformities;
- preparing periodic reports for Corporate Bodies;
- monitoring specific obligations concerning i) customer due diligence, ii) data retention, iii) monitoring transactions, iv) reporting suspicious transactions and (iv) managing risk in a non-EEA context;
- guiding, coordinating and controlling Subsidiaries without centralised management and Foreign Branches.
- providing consulting, advisory and reporting towards the corporate bodies and the structures of the Bank involved in AML related activities;
- defining the specific contents of the training programme concerning anti-money laundering;
- identifying measures and evaluating compliance risks, and managing them via second level controls;
- creating and implementing AML work plan and programs;
- identifying control objectives for first level controls to be performed by business network; analysing the first level control results;
- defining and conducting second level control checks and tests.

With specific reference to customer due diligence obligations, the AML Department carries out the following activities:

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

With specific reference to obligations to retain data, the AML Department carries out the following activities:
- defines the data archive input and management requirements, to comply with anti-money laundering obligations, and checks the reliability of the information system used for data entry, based also on controls carried out by other company entities. More specifically, the AML Department provides assistance in the phase involving analysis of IT activities on said archive and coordinates activities to eliminate any anomalies identified in its management;

With specific reference to obligations on transactions monitoring, the AML Department carries out the following activities:
- prepares and updates the transaction monitoring methods for anti-money laundering, anti-terrorism and embargo management purposes;
- analyses the outcomes of automated transactional monitoring (real-time monitoring of foreign payments; ex-post monitoring of transactions);

- within the scope of managing embargoes, carries out assessments (and oversees the authorisation, as applicable) of transactions ordered by/in favour of customers who are on the Sanctions Lists, on the basis of automatic filtering and following checks carried out by the AML Department;

With specific reference to obligations on reporting suspicious transactions, the AML Department carries out the following activities:
- evaluates suspicious activity reports (both submitted by the network units as well as stemming from the automated transactional monitoring);
- reports to the FIU on transactions considered as suspicious with respect to money laundering, terrorist financing or the financing of programmes for the proliferation of weapons of mass destruction;
- manages obligations related to access of the Authorities, in particular the FIU, the National Bank of Slovakia and the Ministry of Finance.

It also receives reporting from control structures (e.g. Internal Audit and Control Division) and other operational functions (e.g. Network Units) pursuing AML requirements.
As AML IT tool's business owner, provides methodological support to AML IT tool' users.

With specific regard to personnel training, the AML Department carries out the following activities:
- identifies the training objectives and prepares an adequate training programme to ensure that the employees are kept constantly up to date, together with the Human Resources & Organization Department ;
- defines the content of training activities and supports the Human Resources & Organization Department in deciding on how the activities should be carried out.

In the AML Department:
- the Head of the AML Department is given the position of the Head of the AML Department as well as the position of the AML Officer responsible for the suspicious activity reporting.

5.5 AML Officer

The Head of AML Department is entrusted with the role of AML Officer.
The AML Officer and his/her substitute are the persons authorized and responsible for the implementation of measures and actions taken to prevent and disclose money laundering and terrorism financing.

The AML Officer is appointed/removed by the Management Board taken into consideration the opinion of the Supervisory Board. The decision is subject to a binding prior approval by the relevant AFC Head Office Department.

The Head of the AML Department:
- must comply with suitable independence, authority and professional competence requirements and must not have direct responsibilities over operating areas, nor report to the persons in charge of said areas;
- is considered, for all intents and purposes, as one of the heads of the corporate control functions and performs his/her functions independently;
- carries out a supervisory role on the adequacy of the organisation of activities and actual implementation of the internal processes and procedures with respect to anti-money laundering, combat of terrorist financing and managing embargoes within the scope of all the company units, even if said units do not belong to the AML Department. In carrying out that role, and for the applicable profiles, shares the first level control activities to be carried out with applicable operational, business and control entities and their implementation procedures;
- uses the results of the second level controls carried out by the applicable units that belong to his/her Department, and the results that emerge from controls carried out by the Internal Audit and Control Department as part of the third level independent control function;
- monitors the adequacy of internal processes and procedures for the identification, assessment and reporting of suspicious transactions, as part of his/her duty to monitor the effectiveness of the entire management and internal control system overseeing the risk of money laundering, terrorist financing and breach of embargoes.

The Head of the AML Department has a coordination role as regards VUB Group Companies, with overall management of money laundering risk at a VUB Group level.

Furthermore, the AML Officer and his/her deputy perform the following activities:
- prepares AML Guidelines, AML Rulebook and other related procedures;
- carries-out AML self-risk assessment and AML reporting;
- organises and directs AML activities at Bank’s level;
- cooperates with and reports to the AFC Head Office Department in order to ensure the alignment of Bank’s internal AML procedures to the provisions issued by the Parent Bank, in compliance with local regulations;
- reports to the AFC Head Office Department for its evaluation any circumstances, deriving from mandatory local AML Regulatory References, which shall not permit the application of the requirements based on EU Regulation or issued by the Parent Company;
- assesses customers and transactions positively matched against sanction lists, addressing the initiatives required based on the assessment outcomes;
- authorises the opening of ongoing relationships with Politically Exposed Persons and correspondent banking accounts and similar accounts with credit or financial institutions located in third countries identified by the European Commission as high-risk third countries;
- ensures the provision of professional trainings for relevant employees and defines the content of such trainings;
- prepares an annual evaluation of the financial and material resources of the AML Department;
- in his capacity as an AML Reporting Officer, is responsible for reporting of suspicious cases to the FIU;
- provides operating entities with advice on obligations regarding the preparation of suspicious transaction reporting and possible abstention from performing transactions;
- files suspicious activity reports considered as unfounded, providing reasons in writing;

- communicates the outcome of his/her assessment to the Head of the operational entity from which the report originated;
- after being informed, notifies the Head of the operating entity reporting the suspicious transaction that the inquiry has been filed as instructed by the FIU;
- liaises with the FIU and manages requests for further inquiries submitted by the competent authorities;
- manages relations with local authorities;
- submits reports to the Supervisory Board and Audit Committee in line with Operating Rules for Managing Compliance Macro-Processes (Compliance rulebook):
- submits reports to the Parent Company´s relevant AML function in line with Operating Rules for Managing Compliance Macro-Processes (Compliance rulebook)

The Bank shall make available to the AML Officer the following:

- unrestricted access to all the data, information and documentation which is necessary for anti-money laundering and counter terrorism financing;
- adequate authorisation for efficient discharging of his/her duties;
- adequate staff resources both in terms of number and required skills, and also adequate material and other work conditions including remuneration;
- adequate IT solutions and automated tools;
- appropriate conditions which guarantee the adequate level of protection of confidential data and information which are made available to the AML Officer and his/her substitute;
- adequate IT support which makes possible a permanent and secure monitoring of activities in the area of anti-money laundering and counter-terrorism financing;
- regular professional education and training for preventing and detecting of money laundering and terrorism financing;
- substitution to the AML Officer when he/she is absent.

The Head of the AML Department reports directly to the Deputy CEO.

5.6 Risk Management Division

The Risk Management Division carries out activities described in the valid internal documents ID800 THE ORGANIZATIONAL CODE, DISCRETION RULES, SIGNING RULES VÚB, A.S. – annex 2 and in the valid internal procedure No. 807 Integrated Internal Control System Regulation.
Risk Management Division, upon request of AML Department, provides support on the definition of operational and reputation risk assessment methodologies and tools.

5.7 Internal Audit and Control Department

The Internal Audit and Control Department undertakes activities in accordance with the valid internal documents ID800 THE ORGANIZATIONAL CODE, DISCRETION RULES, SIGNING RULES VÚB, A.S. – annex 2 and with the valid internal procedure No. 807 Integrated Internal Control System Regulation.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Internal Audit and Control Department, as part of third level controls of the overall internal control system, monitors the degree of adequacy of the corporate organisational structure and its compliance with applicable laws on an ongoing basis, and also oversees the functioning (in terms of efficiency and effectiveness) and reliability of the risk management model. Specifically, it inspects the adequacy and efficiency of the AML Department at regular intervals and informs the competent Corporate Bodies of the outcome of his/her assessments.

The Internal Audit and Control Department, within the scope of its oversight activities, will ensure *inter alia*:
- constant compliance with due diligence obligations, when establishing customer accounts and during the relationship with the customer;
- the actual acquisition and ordered storage of the data and documents prescribed by applicable legislation;
- the correct functioning of the storage archive of the data and transactions carried out by the customers;
- the actual accountability of employees and business partners, and the managers of central and decentralised units in implementing all the requirements set out under applicable law.

Moreover:
- 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, he/she prepares, on the basis of the findings of the Audit Risk Assessment and the controls performed by the first and second level Functions, the control plan for all the operational entities involved;
- during audits, checks alignment between various management accounting procedures for customer transactions and the data entry and management procedure for the data archive required by anti-money laundering laws;
- it informs the AML Department and other Corporate Bodies of inefficiencies identified during auditing activities and suggests corrective measures to be taken;
- it takes follow-up action to check that necessary corrective measures have been adopted and whether they are suitable for preventing similar critical aspects in the future.

5.8 Human Resources & Organization Department

The Human Resources & Organization Department carries out activities described in the valid internal documents ID800 THE ORGANIZATIONAL CODE, DISCRETION RULES, SIGNING RULES VÚB, A.S. – annex 2.
The Human Resources & Organization Department, upon request of AML Department, provides support on:
- the application of AML requirements when organisational and process changes are planned;
- the definition of correct quantities of resources required to fulfil obligations regarding anti-money laundering;
- the arrangement of employee education, trainings;
- the undertaking of appropriate disciplinary measures, in accordance with regulations, against the employees who have violated their contractual obligations related to AML requirements.

The Human Resources & Organization Department carries out the following activities:
- establishes organisational solutions in line with the objectives and strategies for anti-money laundering, combating terrorist financing and managing embargoes, advised and assisted by the AML Department;
- checks and defines staff numbers, in line with the objectives and strategies of company plans;
- monitors the dissemination of internal regulations and the Bank's governance documentation on anti-money laundering, combating terrorist financing and managing embargoes.

In particular, the Human Resources & Organization Department monitors the analysis and adoption of organisational measures, also arising from new regulatory obligations.

Furthermore, the Human Resources & Organization Department carries out the following activities:

- cooperates, with AML Department in the development of initiatives aimed at disseminating, at all levels of the company, a company culture that is consistent with the principles of compliance with law, and expanding the level of awareness of the possible resulting risks;
- works with the AML Department to carry out training initiatives on compliance,;
- works with the AML Department to define and develop training programmes on an ongoing basis, in order to further technical/professional expertise and update personnel tasked with compliance activities.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Human Resources & Organization Department will also ensure the proper qualitative-quantitative workforce cover needed to meet regulatory obligations.

The Human Resources & Organization Department also :

- assesses and oversees disciplinary actions to be taken against employees who have breached regulations;
- assesses the applicability of the protections established by the collective contracts in the interests of employees involved in criminal, civil and administrative proceedings for alleged breaches of the applicable law and decides on the formulation of the concerns to be resolved when settling the proceedings.

5.9 Business Units and other operational, business and support functions

The Business Units[4] and the other operational, business and support functions have the primary responsibility for managing risks of money laundering, terrorist financing and breach of embargoes: During daily operations, these structures must identify, measure or assess, monitor, and mitigate and report the risks arising from ordinary company operations in accordance with the risk management process set out in the valid internal procedure No. 807 Integrated Internal Control System Regulation ; they must also comply with the operational limits assigned to them in accordance with the risk objectives and the procedures underlying the risk management process.

The operational, business and support functions comply with the company processes and procedures, checking its application with adequate first level controls in order to ensure that the transactions are carried out properly, for the full and complete compliance with applicable rules and standards of conduct. The operational and business entities, in association with the AML Department perform 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 operational, business and support functions are submitted for review by the AML Department that will assess their capacity to actually achieve the control objectives, and if necessary, will request their consolidation.

The operational, business and support functions have a significant role in monitoring risks from money laundering, terrorist financing and the violation of embargoes. For this purpose, they put in place all initiatives aimed at encouraging the diffusion of a culture of compliance with operators, working with them to correctly implement the training programmes defined by the AML Department in association with applicable corporate functions.

[4] Retail and Corporate Banking Divisions

Also:
- the operational and business entities, in line with current service and organisational models, play an active role meeting the requirements of various regulatory frameworks and governed by specific guidelines, processes and internal procedures.

The operational, business and support entities play an active role in meeting requirements relating to anti-money laundering, combating terrorist financing and managing embargoes. More specifically, for the purposes of customers' knowledge, the entities carry out the following activities:
- identify customers as well as beneficial owners, obtain information and documents (including additional information necessary in the case of relations with banks and financial institutions), necessary to carry out the due diligence obligations and assign the customer risk profile;
- take an independent decision on whether to refuse to open an account or execute an occasional transaction for medium risk customers, involving the AML Department, if considered appropriate;
- retain documents obtained and keep relative information updated;
- monitor customer accounts and transactions steadily;
- inform the customers of the Bank's decision not to open an account and/or execute a transaction or of its intention to close an existing account.

Lastly, the operating structures carry out the following activities:
- check *in advance* payments and documents representative of goods, to ensure they conform to provisions of the AML Department as regards transactions with Countries, goods sectors or entities subject to sanctions and/or restrictions;
- check in advance payments ordered by/in favour of customers to verify that they do not have links with the lists of entities known as "Bad Guys", since they are considered to be high-risk on the basis of the profiles assigned by the Group;

5.10 Legal Services Department

The duties and responsibilities of the Legal Services Department are described in the valid internal procedure No. 800 Bank's Organizational Code.

With reference to anti-money laundering, combating terrorist financing and managing embargoes, the Legal Services Department carries out the following activities:
- supports the AML Department in identifying steadily applicable laws, monitoring developments, including case law developments, and providing legal advise to ensure the correct and unique interpretation within VUB Group;
- shares, for legal aspects within its area responsibility, the contents of these Guidelines, internal regulatory provisions and training courses prepared by the AML Department and other assigned entities, formulating proposals for amendments and/or additions;
- advises and assists the AML Department on controversial legal aspects concerning the compliance assessment of internal processes and procedures, contracts, forms or significant cases of inefficiencies that have been identified;
- shares, with the AML Department, standard drafts of notices to be sent to customers regarding the refusal to open an account, or closing of an account or refusal to carry out an occasional transaction.

5.11 Operations and IT Division

The Operations and IT Division carries out activities described in the valid internal documents ID800 THE ORGANIZATIONAL CODE, DISCRETION RULES, SIGNING RULES VÚB, A.S. – annex 2.

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

- cooperates, based on requirements of the AML Department, in coordinating requests regarding activities on IT systems, apart from actions more closely related to anti-money laundering, combating terrorist financing or managing embargoes (e.g. systems for managing the data stored on customer accounts, identifying anomaly indicators, due diligence or risk profiling);
- performs first level controls on the quality of data entered in the data storage archive, addressing any requests for corrective measures to be taken to the relevant IT unit and guaranteeing a periodic information flow to the AML Department, with details of the anomalies found and the progress of corrective actions implemented;
- checks, based on the rules defined by the AML Department, matches with the Sanctions List and/or the internal lists for anti-money laundering and embargo purposes (Bad Guys) resulting from automatic filtering systems and involving the AML Department, if the suspicion is confirmed;
- checks, applying the rules defined by the AML Department, payments and bills of lading if there is a match with the Sanctions List and/or the internal lists for terrorist financing combat and embargo purposes (Bad Guys), involving the AML Department, if the suspicion is confirmed.

Furthermore, with reference to anti-money laundering, combating terrorist financing and managing embargoes, the Operations and IT Division is involved in the development, update and monitoring of application components, carrying out the following activities, to this end, it:

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

5.12 Information Security and Business Continuity Management

The duties and responsibilities of the Information Security and Business Continuity Management Sub-Departments are described in valid internal documents ID800 THE ORGANIZATIONAL CODE, DISCRETION RULES, SIGNING RULES VÚB, A.S. – annex 2.

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

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

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

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

6.1 Definition of guidelines and methodological rules

The Head of the AML Department defines the applicable guidelines and methodological rules to monitor and assess, at VUB Group level, the risk of money laundering, terrorist financing and breach of embargoes.

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

6.2 Risk Assessment and Risk Appetite Framework

The identification and periodic assessment of the risk and related vulnerability constitutes the first logical step in the management model, and helps in the definition of the risk appetite principles and consequent limits to submit for approval to the Management Board 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 Slovak AML Act with implementing provisions on organisation, procedures and internal controls requires recipients to carry out an overall assessment, which is periodically updated, of its exposure to money laundering risk (the so-called self-assessment of exposure to the risk of money laundering).

The Head of the AML Department annually formulates a risk assessment on money laundering, terrorist financing and breach of embargoes (the AML Risk Assessment) for VUB Bank and for the VUB Group, which it submits to the Management Board and the Supervisory Board.

The assessment is carried out on the basis of the methods defined by the Parent Company structures - the Head of the AFC Head Office Department, in accordance with the Head of the Chief Compliance Officer Governance Area and with the help of the Head of the Chief Risk Officer Governance Area of Intesa Sanpaolo. In particular, the AML Risk Assessment methodology surveys the extent of inherent risk and related vulnerabilities, through mainly

quantitative indicators, integrated with qualitative assessments that relate the types of potential risk (e.g. customer risk level, risk level associated with non-cooperative Countries for the purposes of Commission Delegated Regulation (EU) 2019/758) and aspects mitigating the risk of money laundering, terrorist financing and breach of embargoes (e.g. the number of customers whose beneficial owner has been recorded), in relation to the dimensional data of the entity in question.

The risk assessment at VUB Group level result from aggregation of the assessments of the relevant entities of the VUB Group (VUB Bank, VUB Leasing, a.s., VUB Prague) entities. The assessment of the inherent risk, the vulnerability and the residual risk is expressed on a four-level scale, which is the same as the other Corporate Control Functions.

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

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

6.3 Planning of activities

The identification and prior assessment of risks of money laundering, terrorist financing and breach of embargoes and related vulnerabilities is prior to the planning of management interventions, which are submitted, in the context of annual anti-money laundering reports, to the Management Board and the Supervisory Board.

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

6.4 Regulatory alignment

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

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

The AML Department is in charge of continually identifying external laws, with the support of the Legal Department in order to interpret the laws.

The assessment of the impact of applicable laws and consequent proposal of guidelines, rules, processes and procedures is managed by the AML Department, with assistance from the Human Resources & Organization Department, and for legal aspects, from the Legal Department.

The purpose of regulatory alignment is to define *ex ante* a framework for compliance with regulations and laws, based on the following guidelines:
- the guidelines and main strategies to manage the areas with crossover impacts on VUB Group operations are defined in specific guidelines that need to be approved by the Management Board;
- the rules governing relevant areas are set out in documents that describe the methodological aspects, operational mechanisms, rules of conduct and mandatory restrictions to comply with, also implementing the guidelines and in compliance with the policies contained therein;
- the processes, where standardised, are supported by IT procedures and instruments that can assist and guide the behaviour of the staff, in order to ensure they behave correctly;
- in the more sensitive processes, the guidelines and rules of other Bank structures provide for the prior involvement of the AML Department;
- the processes establish a system of controls which can effectively monitor the effectiveness of the controls over time, even taking into account the legal and business evolution.

6.5 Advisory and clearing

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

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

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

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

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

The assessments of the AML Department are carried out using formats that, as far as possible, are defined to include the following:
- the subject of the assessment;
- the applicable internal and/or external regulatory context;
- the main aspects to analyse, which are significant for assessment purposes;
- brief considerations, identifying the level of consistency with the spirit and letter of the law and internal regulations, any residual risks and recommendations.

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

6.6 Assurance

6.6.1 The assurance model

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

In line with the valid internal procedure No. 807 Integrated Internal Control System Regulation provisions with respect to risk monitoring and control, the assurance model assigns:
- the line controls to the operational, business and support entities, carried out on a continuous basis over individual transactions, and the managerial analyses consisting of the systematic monitoring of phenomena characterised by high anomaly levels that have to be promptly dealt with, and/or reported to a context of operational and management uniformity;
- to level-two control functions the monitoring of the correct adoption - by operational, business and support entities - of the applicable methodological and control framework, through verifications on the design of processes, procedures and on the actual and correct adoption of required controls.

The model defined to create the risk assurance process relating to the risk of money laundering, terrorist financing and breach of embargoes provides for the following:
- during the definition of the review of company processes, also following changes to the external legal context, the AML Department establishes the control objectives to mitigate the risk of money laundering, terrorist financing and breach of embargoes, notifying the operational, business and support structures, as well as competent organisational structure;

- the operational, business and support structures, upon guidelines provided by the AML Department perform the first level controls that they believe are capable of actually achieving the control objectives, and implement them. The first level controls performed by the operational, business and support structures are submitted for review to the AML Department, that will assess their capacity to actually achieve the control objectives, and if necessary, will request their consolidation;
- the AML Department on the basis of an assessment of the process defined in that manner and the results of the first level controls, will define and carry out the second level controls; these controls may be remote, checking the performance of monitored events, or on-site controls of processes adopted by operating structures and their effectiveness, as well as controls on the correct performance of level-one controls by operating structures; depending on the level of risk identified, and taking account of capacity limits , the frequency of controls may be continual or periodic, or inter-annual, annual, or long-term, or on a *una tantum* basis.

6.6.2 Method for carrying out activities

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

The *una tantum* second level controls, mostly relating to checks on the processes and/or phenomena considered to be significant, are planned by the AML Department, on an annual basis, taking account of the results of the AML Risk Assessment and/or other signs (for example findings by the Supervisory Authorities or the Internal Audit and Control Department, specific requests of the Corporate Bodies).

The AML Department reports these controls to the CEO Deputy and if relevant to the operational, business and support structures; this reporting must be based on a format defined beforehand, as far as possible, and must include:
- the characteristics of controls (the subject, the applicable internal/external regulatory context);
- details of controls carried out and relative outcomes;
- brief considerations, indicating residual risks and mitigation actions suggested.

Individual organisational units are responsible for planning and adopting corrective actions; the above-mentioned AML Department monitors and tracks the progress of actions identified.

6.6.3 Interaction with other control functions and information flows

The collaboration methods between the Corporate Control Functions and the relative information flows are set out in the valid internal procedure No. 807 Integrated Internal Control System Regulation.

In carrying out the checks, the AML Department also use the results of checks by the Internal Audit and Control Department, who make the necessary assessments on the processes and behaviour, making the relative results available to the units in charge of monitoring.

Additionally, in order to ensure the ongoing effectiveness and validity of the control systems monitoring the risks of money laundering, terrorist financing and breach of embargoes, the first, second and third control level Functions take part, to:
- get more in-depth information on the findings from the control activities, encouraging the standard and integrated assessment of the risks in question;

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

The AML Department has access to all the Bank activities and any relevant information to carry out their duties, including through direct interaction with the staff. To this end:
- they receive and send the information flows reported in the valid internal procedure No. 807 Integrated Internal Control System Regulation;
- the other company structures must inform them, in a timely and complete manner, of any relevant facts in order to monitor the risks in question;
- they may request and receive any other relevant information to carry out their duties from the other company functions.

6.6.4 Follow-up process

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

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

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

The AML Department works with the Human Resources & Organization Department to establish efficient channels of communication and training instruments, identifying relative training requirements and preparing the content of training initiatives for all the Bank resources, in order to ensure that staff, with specific attention paid to the sales staff and the heads of the business structures, have adequate awareness of applicable laws, obligations and related responsibilities, the consequences resulting from failure to fulfil said obligations and to ensure they are able to knowingly use supporting instruments and procedures in meeting requirements established by law.
The AML Department, with the assistance of the Human Resources & Organization Department monitors development of the training programmes, checking its use and effectiveness, and provide adequate results to the Corporate Bodies, also for the timely identification of any action that may need to be taken.

In addition to traditional training activities, the AML Department, in association with the Human Resources & Organization Department, organises and takes part in specific initiatives aimed at disseminating a culture of risk and expanding the level of awareness of the approach to risk requested, including in particular:
- induction sessions for Company Bodies and workshops for senior management on particularly delicate or topical issues;

- actions to make the operational, business and support structures more aware of the specific risk aspects involved in ordinary operations;
- diagnostic activities in order to understand the level of diffusion of the risk culture at all company levels, in terms of consistency of perceptions and conduct with respect to required guidelines and policies.

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

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

The management of relations with the Authorities and non-compliance events is an extremely important part of the control of compliance risk. The AML Department provides for management of the following in the areas it is responsible for:
- relations with the Supervisory Authorities, coordinating activities necessary to follow up requests from the Authorities;
- non-compliance events, assisting and working with the unit involved, to ensure the identification and implementation of actions to take to bridge any organisational and/or procedural gaps.

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

6.9 Specific requirements

6.9.1 Customer Due Diligence

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

Based on the level of risk attributed to the customer, the following approach to due diligence is adopted:
- ordinary obligations;
- simplified obligations;
- enhanced obligations.

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

If it is not possible to comply with customer due diligence obligations, an account cannot be opened, a transaction cannot be carried out, or an assessment of whether to close an existing

account must be made. In these cases, the sending of suspicious activity reporting must be considered.

Customer due diligence obligations are met through:

- identifying the customer, any executing party and beneficial owners, and checking the identity of these subjects: the identification is based on obtaining identification documents, documents certifying due diligence issued by other intermediaries and any additional information required to establish the risk profile to be assigned to the customer; assessing the identity of subjects based on documents, data and information obtained from a reliable and independent source;
- customer profiling based on the risk of money laundering, terrorist financing and breach of embargoes: profiling is based on assigning a score - produced from data and information obtained when opening an account and monitoring activities - and the consequent classification of customers into four bands, depending on whether the risk is considered as high, medium, low or insignificant; in the case of medium or high risk customers, enhanced due diligence obligations apply; profiling is subject to a harmonisation process at a Group level, based on which each Company of the Group undertakes the highest risk profile from those assigned by other Group Companies for the same customer[5];
- authorisation to open a new account, execute an occasional transaction or maintain an existing account on the basis of the risk profile assigned to the customer: for high or medium risk customers, to whom enhanced due diligence obligations apply, authorisation is issued: (i) for high risk customers, by the AML Department, based on previously established, objective criteria; (ii) for medium risk customers, by the operating structure. With reference to Politically Exposed Persons, an authorisation procedure is started with specific authorisation from the AML Officer / Deputy AML Officer;
- authorisation or refusal to proceed, issued by the AML Department, for customers, who, during the collection of information or updates of the register, are found to be on the Sanctions Lists, also following checks carried out by the applicable functions of the VUBL Operations Department;
- the periodic review of the risk profile: for customers with a high or medium risk, the relationship is reviewed, every 18 and 24 months[6], apart from Politically Exposed Persons, whose data and banking relations are reviewed every 18 months, regardless of the risk associated with the customer; besides this frequency, the following events require the classification of subjects with a high or medium risk and, if the score increases, the updating of data on due diligence and a review of the position: i) acquiring the status of Politically Exposed Person; ii) reporting suspicious activity; iii) notification of a criminal investigation.

Under no circumstances may due diligence obligations be assigned to shell banks or intermediaries established in high risk third Countries[7] or whose local laws prevent adequate monitoring of the risks of money laundering or terrorist financing and, in particular, the sharing of data and information relative to own customers, within its own group.

6.9.1.1 Ordinary due diligence obligations

For customers without a high or medium profile related to risk of money laundering and terrorist financing, classified as having an immaterial or low risk, ordinary due diligence obligations apply, consisting in identifying the customer, any executing party and beneficial owner,

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

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

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

checking the identity of subjects referred to, based on documents, data and information obtained from a reliable, independent source, and obtaining and assessing information for this purpose and on the nature of the ongoing relationship or occasional transaction, and carrying out continuous controls on the account/relationship.

6.9.1.2 Remote transactions

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

In this regard, the Bank:
- obtains identifying data regarding the customer and any executing party and their correspondence on a copy – obtained in an electronic format or with similar procedures - of valid identity documents pursuant to applicable legislation; and

obtains additional information, concerning the process of identifying the customer, according to a risk-based approach, through one or more of the following measures: (i) transfer made by a customer through a banking and financial intermediary established in an EU member country, (ii) findings based on solutions with secure forms of biometric recognition.

6.9.1.3 Simplified customer due diligence

In the case of a low or insignificant risk of money laundering or terrorist financing, due diligence obligations may be simplified, reducing the extension and frequency of ordinary obligations. This category, unless otherwise determined ad hoc regarding a specific customer, comprises the following customer categories:
- banking and financial intermediaries, excluding traders, insurance intermediaries operating in the life sector, trust companies, financial advisors and financial consulting companies;
- companies listed on regulated markets and subject to the disclosure obligations that include ensuring adequate transparency of beneficial owners;
- public administrations, institutions or bodies that perform public functions conforming to European Union law;
- banking and financial intermediaries in the EU or with their headquarters in a non-EEA country adopting an effective system to combat money laundering and terrorist financing, based on indicators used to determine such risks.

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

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

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

6.9.1.4 Enhanced customer due diligence

Enhanced due diligence applies to customers classified as high risk, in medium or high risk range. The following are always considered as high risk:
- particular types of accounts and transactions:
  - accounts and occasional transactions involving high-risk third Countries[8];
  - correspondent accounts that involve payments, and similar accounts with credit and financial institutions established in a non-EEA country;
  - transactions with unusually high amounts, or for which there are doubts as to their purpose;
- special types of customers:
  - Politically Exposed Persons;
  - other types of customers considered as high risk, such as: trusts, local and foreign money transfer companies that undertake cash remittances, agents in Slovakia and abroad of Slovak and Foreign Financial Institution, Money Transfer Institutions that undertake cash remittances, betting operators, trust companies that are not part of the Intesa Sanpaolo Group, regardless of whether they are registered in the register of trustees, foreign financial or credit intermediaries not subject to the authorization to carry out the activities by the Supervisory Authorities of the country where the principal place of business is established and additional types of customers as outlined in valid internal procedure no. 660 AML Program (PROCESS „KNOW YOUR CUSTOMER“).

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

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

correspondent accounts with banks or financial institutions having their principal place of business in non-EEA Countries, specific authorisation by AML Officer / Deputy AML Officer.

6.9.2 Record keeping

The data recorded in the course of customer due diligence shall be kept for ten years after the termination of the business relationship or the performance of the transactional order in line with valid internal procedure No. 414 “Processing, storage and safe-keeping of banking documentation”, i.e.:.

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

6.9.3 Transactions monitoring

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

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

- *ex ante* monitoring, by the operational structures that carry out the transactions, to identify, block or report those suspected of money laundering, terrorist financing or breaching regulations on embargoes, and regarding the limitations of use of cash and bearer-negotiable instruments. The operating structures may be assisted by the AML Department to assess whether there are grounds to refrain from carrying out a transaction. If there are grounds, the operating structures notify the AML Department, so that it may assess whether to not carry out the transaction and request the FIU to issue a suspension measure in case of evident risk;
- *ex ante* control of the payments and documents representing goods by checking them against the Sanctions Lists and/or the internal Group lists (Bad Guys) and checking the findings from the control procedures. These checks are automated and involve the Payments sub-department and the AML Department; The traceability of controls on transactions originating from/for Countries, persons and entities against whom restrictions have been established involves the business and operating structures that perform the transactions, which require authorisation from the AML Department to go ahead with the transactions;
- *ex post* monitoring of the transactions by the AML Department in order to identify anomalous transactions, including with the assistance of the automatic anomaly indicators management system (where provided for).

Furthermore, in order to reduce the risk of money laundering, terrorist financing and breach of embargoes, and the related reputational, legal and operational risks, taking into account specific regulations on the matter, the Intesa Sanpaolo Group (i) does not make “cover”

payments[9] in United States Dollars and (ii) operates with payable-through accounts[10] only on condition that customer due diligence is guaranteed by the counterparty bank using said payable-through accounts[11].

6.9.4 Reporting of suspicious transactions

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

- first level reporting by the Heads of the company business structures and / or other company structures, who have to immediately report any transactions of this nature that they discover to the AML Department;
- second level reporting by the company units identified in the AML Department, who examine the reports received and, if considered warranted, send them to the Financial Intelligence Unit (FIU). Reports on transactions considered suspicious with respect to money laundering, terrorist financing or financing proliferation programmes for weapons of mass destruction coming from the operational structures fall under the above-mentioned examination.
- reporting of suspicious activity reports in terms of the automated *ex post* monitoring of the transactions by the AML Department

6.9.5 Risk management in a non-EEA Countries context

The Bank shall be compliant with the provisions of Commission Delegated Regulation (EU) 2019/758 that establishes for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries (non-EEA countries).

6.10 Information flows to Corporate Bodies

The Bank is liable to the provisions of AML Regulatory References, and it is therefore obliged to set up processes of reporting to the FIU and Bank corporate bodies aimed at preventing of money laundering and terrorism financing and dealing with embargoes. The content of reports depends on which organisation it is intended for and also on the purpose of reporting, as follows:

- external reporting to supervisory bodies in accordance with requirements established in money laundering prevention and embargoes regulations (i.e. FIU, Ministry of Finance, National Bank of Slovakia);
- reports on AML activities addressed to the Supervisory Board, to the Management Board, to the Audit Committee and the AFC Head Office Department as outlined in Rules for Managing Compliance Macro-Processes (Compliance rulebook) in the sections relative to the duties of AML Officer.

[9] 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.

[10] 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.

[11] In particular, in the case of a correspondent account with a non-EEA credit entity, the Bank must ensure that it has checked the identity of customers with direct access to transition accounts, that is has met customer due diligence obligations and, on request, may provide the data obtained in meeting such obligations.

7 GROUP GOVERNANCE

Considering its operational and territorial base, the VUB Group systematically adopts (where applicable) a unified approach to anti-money laundering, combating terrorist financing and managing embargoes, with guidelines, rules, processes, controls and IT instruments that are reasonably standard at VUB Group level.

Within the VUB Group, taking account of the VUB Group's operating and local structure, the governance process involves:

- VUB, a.s., Prague branch
- VUB Leasing, a.s.

VUB Bank is responsible for ensuring that the Guidelines issued by VUB Bank are distributed to the subsidiary and to the branch and verifying their correct adoption and application. The information flows sent to VUB Bank must provide suitable information on the compliance situation at subsidiaries, with reference to risks concerning anti-money laundering, combating terrorist financing and managing embargoes.

7.1 The direction, coordination, and control model

The Bank applies the steering, coordination and control model. In this regard, the AML Officer

- inform the AFC Head Office Department, in full and as promptly as possible, about the outcomes of control activities carried out based on the control macro-objectives provided by the Head of the AFC Head Office Department, as well as any significant event. In this regard, it also provides half-yearly reports on issues governed by the guidelines set forth by the Parent Company[12];
- propose and/or share remedial actions to adopt for shortcomings identified, defining the relative times and responsibilities for implementation. In this regard, on a monthly basis, the AFC Head Office Department is notified of the progress of activities;
- work with the Supervisory Authorities in order to be updated on the regulatory framework and operate in compliance with applicable provisions relative to the business model adopted and/or Slovakia, coordinating with the AFC Head Office Department, with a view to acting consistently with Group Guidelines and facilitating dialogue with the Authorities. The AFC Head Office Department assists the VUB Group in establishing relations with the Authorities, without prejudice to the responsibility of the VUB Group to implement the specific regulatory requirements of the business sector and/or Slovakia;
- promptly informs the AFC Head Office Department if local laws do not permit the adoption of measures to combat money laundering, terrorist financing or to manage embargoes that are equivalent to those of the European Union, so that the Head of the AFC Head Office Department may inform the Bank of Italy pursuant to Italian Legislative Decree no. 231/2007.

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

The Head of the VUB AML Department transmits to the Group Delegate a copy of suspicious activity reports sent to the FIU or to the competent Foreign unit,[13] and those filed, complete with motivation of said decision, without prejudice to local rules governing banking and/or

[12] For example, these issues may concern developments in the local regulatory context, the number and type of transactions reported, the number and type of high risk customers accepted, training programmes scheduled and delivered, breaches of provisions found, objections received from the competent authorities.
[13] Article 33, paragraph 2 of Directive (EU) 2015/849 requires the party obliged to report the suspicious transaction to send information to the Unit of the Member State where it is situated.

professional secrecy, as well as any local provisions that prevent the transmission of these notices to the Group Delegate. The transmission of information is carried out using procedures designed to guarantee maximum confidentiality of the identity of the first level Manager making the report. In order to investigate anomalous transactions and accounts at a Group level, the Group Delegate may be assisted by all Company structures.

The AFC Head Office Department sets out the Group guidelines and oversees their correct adoption. For this purpose, with reference to profiles related to the management of risks of money laundering, terrorist financing and breach of embargoes, the AFC Head Office Department:

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

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

The VUB Group is required to:

- adopt guidelines and rules issued by the Parent Company on managing risks of money laundering, terrorist financing and breach of embargoes, aligning them, where necessary, in coordination with the AFC Head Office Department, to their own context and specific aspects of local regulations;
- adopt the operating working standards and methods defined by the AFC Head Office Department, agreeing on any adaptations to reflect the specific situation of the company;
- give the AFC Head Office Department with reference to anti-money laundering, combating international terrorist financing and embargoes, the information flows defined the VUB Compliance Guidelines, also guaranteeing prompt information in the case of events that may cause the risks related to this sector to emerge.

The information flows sent to the Parent Company must provide suitable information on the compliance situation belonging to VUB Group at subsidiaries, with reference to risks concerning anti-money laundering, combating terrorist financing and managing embargoes.

7.2 VUB Prague

VUB Group AML Guidelines, as a framework document, is applicable to and binding for VUB Prague, adapted to its business model, and is referenced in the valid internal document no. 905 System of Internal Principles, Procedures and Control on Measures and Actions for Anti-Money Laundering and Counter-Terrorism financing.
The fulfilment of legal and regulatory requirements in terms of methodology and professional training ensures the VUB AML Department.

The role of the AML Officer is assumed by the Head of Legal and Compliance. The AML Officer of VUB Prague reports hierarchically to the VUB Group AML function and has the authority to report suspicious transactions towards the Czech FIU (FAU).

In line with the Act no. 253/2008 Coll. on measures against money laundering and terrorist financing and the Regulation of the Czech National Bank no. 67/2018 Coll. on requirements on the internal control principles, procedures and control measures against money laundering and terrorist financing and in line with valid directives of the EC, VUB Prague adopted an internal procedure setting procedures against money laundering and terrorist financing (internal document no. 905 as stated above).

7.3 VUB Leasing

VUB Group AML Guidelines, as a framework document, is applicable to and binding for VUB Leasing, adapted to its business model, and is referenced in the valid internal procedure no. 448 VUB Leasing (Policy AML Program – prevention of money laundering and terrorist financing).
The fulfilment of legal and regulatory requirements in terms of methodology and professional training ensures the Operations Department and the Legal team of VUB Leasing in cooperation with the AML Department and the Human Resources & Organization Department of VUB Bank. Daily tasks are assigned to appointed employees of the Operations Department and the team Legal services.

The role of the AML Officer is assumed by the director of the Operations Department, who is appointed by the Management Board of VUB Leasing. The role of the Deputy AML Officer is assumed by a senior lawyer from the Legal team, who is also appointed by the Management Board of VUB Leasing. The AML officer and his/her Deputy report directly to the CEO of VUB Leasing. The appointment, removal and incentives and promotions (in terms of objectives setting, results evaluation and bonuses definition) of VUB Leasing AML Officer are subject to a binding opinion of the VUB Group AMLO.

The AML Officer of VUB Leasing has the authority to report suspicious transactions towards the FIU.

The valid internal procedure no. 448 VUBL - AML program – prevention of money laundering and terrorist financing outlines the control framework of VUB Leasing as obliged person aimed at prevention of money laundering and terrorist financing in line with the requirements of the Act no. 297/2008 Coll. on prevention of money laundering and terrorist financing and of the Act no. 186/2009 Coll. on financial intermediation and financial advisory.
VUB Leasing is obliged to update the AML program not only following legal and regulatory changes but also following changes related to proper business performance and or organisational changes. The updates of the AML program are subject to approval by the Management Board of VUB Leasing.

8 FINAL PROVISIONS

This Document shall be acknowledged by the Supervisory Board of the Bank, in agreement with the Parent Company's relevant AML Function.

As a result of risk assessments and decisions made by the AML Officer or the Supervisory Board, this Document can be amended if the purpose of effective money laundering prevention would reasonably require it.

8.1 This internal document repeals:

Internal document 743 VÚB BANK AML GUIDELINES ON MEASURES AND ACTIONS FOR ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING, version 3, effective from 01.03.2019

8.2 This internal document relates to:

- Internal document No. 742 VÚB Bank AML RULEBOOK for the Fight Against Money Laundering and Terrorism Financing and the Handling of Embargoes, valid
- Internal document No. 660 AML Process "Know Your Customer" in VÚB, valid
- Internal document No. 913 Operating Rules for managing compliance macro-processes (Compliance Rulebook), valid.