

AML / CFT in UBI><Banca

**Organisational model, regulatory framework
and management policies**

AML – CFT in UBI Banca - introduction

The prevention of money laundering and terrorism financing risks in UBI Banca Group is managed in full compliance with the current European and Italian regulations¹ and with the implementing provisions (“Provisions”) issued by the Bank of Italy (the Italian Central Bank, member of the European System of Central Banks (ESCB) and of the Eurosystem).

Risk management policies for the prevention of money laundering and terrorist financing and the related organisational model are part of the increasing attention towards organizational and internal control issues that characterize the Group's regulation, in the assumption that efficient organisational and governmental structures represent an essential condition in order to prevent and mitigate business risk factors.

In particular, there is a special focus on:

- a clear definition, at different levels, of roles, duties and responsibilities;
- the implementation of procedures designed to ensure compliance with customer due diligence obligations, suspicious transaction reporting requirements and retention requirements concerning documentation and records of accounts and transactions;
- the maintenance of a special department in charge of supervising the commitment to prevent and counteract the aforementioned risks;
- the coordination of control departments, also through adequate information flows in order to facilitate the sharing of relevant information and prevent inconsistencies between the different sources of information; at the same time, the Group aims to ensure that the architecture of the control departments is proportionate to the organisational structure, its complexity, the size of the company, the type of services and products offered and to the risk profile referred to the customers' characteristics;
- monitoring that staff and collaborators respect the internal procedures and the regulatory obligations, especially regarding the matters of an "active collaboration", customer and beneficial owner due diligence and ongoing monitoring of the business relationships;
- the empowerment of employees and external collaborators, also with their participation in training programs.

Regarding this last point, it is important to highlight that anti-money laundering department handles the training of employees on contrasting money laundering and the financing of terrorism, on a continuous and systematic basis.

To that goal, together with the competent structures of the Parent Company, the Banks and the Subsidiaries, it carries out:

- an analysis of the training needs, which must take into account any provision of the legal framework, the specificity of the different business roles and the past initiatives that involved employees;
- the design, development and continuous update of the contents of training initiatives, with a

¹ - Directive UE 2015/849 of the European Parliament and the Council (the “fourth Directive”), implemented in national law by Legislative Decree n. 109/2007 and subsequent amendments and by Legislative Decree n. 231/2007 and subsequent amendments.

unitary approach inside the whole Group;

- the planning of training delivery on a risk-sensitive bases, considering the risk exposure in every Bank, Subsidiary and in each of their organisational units, assessing the relevance of the different risk factors in place.

The education and training of the employees ensure an adequate culture of the staff and collaborators who are more in contact with customers and of the personnel belonging to the anti-money laundering Department and to the suspicious transaction manager's Department. These employees are required to be regularly updated about the development in the money laundering risk scenarios and about the typical patterns of criminal financial transactions.

A more in-depth examinations are given in the following sections:

1. The organisational model,
2. Management of money laundering and terrorist financing risks.

1. The organisational model

In order to enhance the management of risks of money laundering and terrorist financing and to fulfil the legal requirements in terms of organisational measures, procedures and internal controls, UBI Group adopted an organisational model that entrust UBI Anti-Money Laundering & Investigations with the governance of the activities related to anti-money laundering and finance of terrorism legislation.

Following the adoption of the one-tier management and control system, since 12 April 2019 the department, covering the role of UBI Anti-Money Laundering Unity, reports directly to the Chief Executive Officer, maintaining a functional report to the Board of Directors.

Within Group's Banks and Subsidiaries, in consideration of the peculiarities of the different subsidiaries, there are two organizational models of the anti-money laundering structure:

1. Banks and subsidiaries which have outsourced the anti-money laundering activity to the Parent Company: in these cases it is appointed an AML Representative who, working in close functional coordination with the Parent Company structure, is in charge of the management of the processes linked to the legislation, with the support of its reference structure, if provided. In particular, the AML Representative carries out the business in accordance with the instructions issued by the AML department in order to ensure the operational consistency within the Group regarding the management and assessment of money laundering and terrorism financing risks.

2. Banks and subsidiaries which haven't outsourced the anti-money laundering activity to the Parent Company: in these cases it is established an Anti-Money Laundering Department, in charge of identifying and implementing adequate procedures addressed to manage the Risk, and it is appointed a specific Officer who, working in accordance with the guidelines received from the Parent Company, is in charge of monitoring the proper functioning of procedures, organizational units and systems and also of providing advice and support risk management choices.

The Manager of UBI Anti-Money Laundering & Investigations Area acts as the Anti-Money Laundering Chief Officer for UBI Banca and for the banks and subsidiaries that outsourced the activity to the Parent.

In the other banks/subsidiaries responsibility is assigned to the Officer of the local anti-money laundering department (Anti-Money Laundering Chief Officer).

Furthermore, considering the role of direction, coordination and control of the Parent Company towards the other Banks and Subsidiaries, UBI Anti-Money Laundering Manager also fulfils the role of Group Anti-Money Laundering Manager, to whom is attributed the whole management of the anti-money laundering risk at Group level.

Concerning the detection and reporting of suspicious transactions to the Financial Intelligence Unit, UBI Banca Group has appointed UBI Suspicious Transaction Manager as Delegate (from now on “Group Delegate”) both for UBI Banca and for the Group on the matter of suspicious activity reporting.

Banks/Subsidiaries which haven’t delegated the Group Delegate, appoint their own Suspicious Transaction Manager who sends to the Group Delegate due information regarding suspicious transactions and control activities carried out.

UBI Suspicious Transactions department has a role of supporting staff of the Board of Directors.

The Suspicious transaction’s Manager is responsible for:

- a) evaluating, in light of all the available elements, the suspicious transactions received from a branch Manager or any other operating point, organizational unit, or departments in charge to manage business relationships with the clients (so called “first level”), or of which he became aware in the exercise of his daily activity;
- b) reporting to the FIU the reports which are deemed to be truthful, without disclosure of the names of the people involved in the procedure of reporting of the suspicious transaction;
- c) maintaining evidence of the assessments carried out under the procedure, even in cases of non-transmission to the FIU of the reports;
- d) carrying out random verifications within his control activities on the adequacy of assessments conducted by the first level analysing structures of customers’ operations.

2. Management of money laundering and terrorist financing risks

The current internal regulation on the matter of preventing money laundering and terrorist financing is mainly organized on two hierarchically linked levels:

1. “Policy and governance Regulation for the management of risks connected with money laundering and terrorist financing”,
2. “Anti-Money Laundering Regulation Handbook”, the so called Anti-Money Laundering Guidebook, to be written by the anti-money laundering department.

The internal regulation is published and can be consulted online by all Staff on the “Regulatory Portal”, accessible on the corporate intranet, and its contents are also used for training initiatives delivered to all Staff.

The requirements contained in the document “Policy and governance Regulation for the management of risks connected with money laundering and terrorist financing” represent an important part of UBI internal control system. Such provisions implement the “Guiding Principles of the Internal Control System of UBI” in the context of preventing the risk of money laundering and terrorist financing (hereinafter “Risk”/“Risks”).

In the context of the control system in place to manage the risk, the Group uses also Data Analytics technologies that, alongside with the adopted tools, allow to extract from data acquired throughout the course of the relationship, useful information for the effective functioning of safeguards provided for.

In order to address the risk management activity within the Parent Company and in the Subsidiaries and to ensure and maintain over time high level of compliance, the document defines:

- the guidelines and general guiding principles;
- the management guidelines, also by identifying cases – further than those provided for by law – for which any transaction is prohibited;
- the characteristics of the organisational model adopted, in accordance with criteria, principles and guidelines. In particular, the organisational model determines:
 - the main roles and responsibilities attributed to the parties involved in anti-money laundering and terrorist financing activities;
 - the representation of the main processes related to the prevention and management of money laundering and terrorist financing risks, also with regard to the assessment of compliance;
 - the description of the main relations and information flows within the Group units involved;
 - the definition of the reporting model.

“Anti-Money Laundering Regulation Handbook”, addressed to all Staff, establishes the rules set out by the Group in order to apply the regulation on the aforementioned matter, summarizing in a single document the company rules and the instructions to follow when performing operations.

The Handbook is divided into five sections containing regulatory and operating instructions provided to enforce the law requirements and structured as follows:

- I Section Legal Framework, providing a general overview on the matter of the regulatory framework;
- II Section Customer Due Diligence;
- III Section Limitations to the use of cash and bearer instruments;
- IV Section Record retention data requirements;
- V Section Suspicious transaction reporting requirements;

In particular:

- I and V Sections are addressed to all Banks and Group's subsidiaries obliged to comply with anti-money laundering and terrorist financing legislation;
- II, III and IV Sections are mainly directed to Banks and Group's companies working on the basis of the operational processes and on the functionalities of the Target IT System;
- other Banks and Group's Companies must take any action in order to update their operating provisions and to adapt their IT systems in compliance with the instructions given by UBI within its role of guidance, coordination and control, among which are included the provisions periodically provided with Group's interoffice circulars.

It is important to underline that the Group has developed an "Anti-money laundering Portal", a monitoring tool created to analyse those events which require a deeper investigation due to the importance of the underlying transaction or to focus the attention on the approaching of a deadline requiring further operations pursuant to internal regulations. "Anti-money laundering Portal" coordinates and supports the activities of the network departments and it is a fundamental tool to carry out a second level verification on the operational units' work.

The Anti-money laundering Portal's Handbook contains the operational instructions on the use of the tool.

All staff is required to strictly comply with the provisions established in the Handbooks and as amended by any follow-up interoffice circulars, having awareness that failure to comply with them in their daily activities might lead to criminal and administrative sanctions established by law.

The results of the ordinary and extraordinary management of operations and projects connected to the prevention of money laundering and terrorist financing are periodically disclosed to the management board, supervisory board, and other strategic general management bodies of the Group.