BANCA VALSABBINA

Anti-Money Laundering Manual

Part 0 – Policy

Approved by the
Board of Directors
on 4 December 2013

TABLE OF CONTENTS

1. POLICY PURPOSE

The Bank of Italy Circular no. 263 dated 27 December 2006 ("New provisions for banks' prudential supervision"), with the 15th update dated 2 July 2013, defines a systematic principles and rules framework for intermediaries to which the internal control system and the corporate bodies' general organisation principles, roles and tasks must aspire.

The intermediaries define and approve strategic guidelines and a business model, while fully aware of the risk detection and assessment methods, and the risks to which these choices expose them.

° ° °

The Policy's purpose is to collect the guiding principles adopted by the Bank to prevent money laundering and terrorism financing risks, to which the specific parts of the Anti-Money Laundering Manual are dedicated.

This Policy is structured as follows:

- strategic guidelines and government policies;
- organisational and control measures to mitigate the risk;
- customer knowledge and adequate verification;
- the duty to abstain;
- active cooperation in detecting anomalies.

2. STRATEGIC GUIDELINES AND GOVERNMENT POLICIES

1.1 10 MARCH 2011 BANK OF ITALY PROVISION

The 10 March 2011 Bank of Italy Provision prioritised the involvement of Corporate Bodies in the mitigation of risks related to money laundering and international terrorism financing which involve sanctions and reputational damage.

Corporate bodies must:

- define company policies which are consistent with anti-money laundering principles and rules;
- adopt specific policies to protect the company's integrity against money laundering risks.

1.2 GUIDELINES

The Board of Directors encourages the Bank to follow these guidelines:

- Opposition to money laundering is an ongoing challenge - Alongside the relevant institutions, the Bank is actively involved in this fight. While strict, clear and incisive rules are necessary, they are insufficient because crime is continuously looking for new ways to launder the proceeds of its illegal activity by exploiting the opportunities allowed by globalisation and by technological and financial innovation. This requires a high ability to recognise innovative tools, methods and circuits used by crime to circumvent risk prevention restrictions;

- The risk-based approach is the most efficient way to conduct the prevention - According to this principle, the Bank's defences must be correlated to a specific risk, which depends on the nature of the subject, the products and services provided, and the specific situations. The principle permits the autonomy of intermediaries, while making them responsible for applying the proper level of control;

- Burdens related to anti-money laundering legislation are lower than the benefits - It is sufficient to consider risk reduction, greater security and the strengthening of trust with customers, which may result from successful action to combat crime;

- The correct application of the requirements is essential - It ensures the proper legal compliance and protects the Bank (under ex Legislative Decree no. 231/01 - Administrative Responsibility of the Entity) and/or employees from serious pecuniary administrative penalties.

3. ORGANISATIONAL AND CONTROL MEASURES TO MITIGATE RISK

3.1 10 MARCH 2011 BANK OF ITALY PROVISION

The 10 March 2011 Bank of Italy Provision assigns the following responsibilities to corporate bodies:

- Putting in place any organisational and operational measures which avoid the risk of money laundering and terrorism financing;
- Carry out regulations compliance controls and adequate risk management.

3.2 GUIDELINES

The Board of Directors encourages the Bank to follow these guidelines:

- Focusing on money laundering prevention is a constant operational practice - It must permeate all production processes and goes beyond a purely formal approach;

- Continuous training strengthens the corporate culture - Trust in the rules and the internalisation of the values that they aim to protect, must precede the rule's application so that such compliance is not just an operational act;

- Line controls are the best tools to intercept and prevent the risk - The correct functioning of the line controls, and the related IT supports, are the best guarantee against money laundering;

- A dedicated centre - The specialised anti-money laundering department provides a dedicated service to develop the company's prevention culture and ensure consistency between the various processes;

- Operational checks are the only things which can ascertain the system's operation level – A specialist anti-money laundering supervision, based on proportionality and effectiveness, ensures the prevention system's efficiency along with targeted operational checks.

4. CUSTOMER KNOWLEDGE AND ADEQUATE VERIFICATION

4.1 3 APRIL 2013 BANK OF ITALY PROVISION

The 3 April 2013 Bank of Italy Provision introduced more stringent verification requirements, insisting that intermediaries:

- adopt transparent and objective evaluation systems and decision-making processes, which are periodically verified and updated;
- define the risk classes beforehand;
- assign a specific risk profile to each customer which is consistent with the previously determined risk classes. This profile shall be based on the information acquired and analyses carried out based on the customer's ongoing relationship and the type of transaction (so-called evaluation criteria);
- set the updating frequency of the customer profiling, based on the related level of risk and events or circumstances that are likely to change over time;
- use a structured procedure for the collection of data and information which can automatically process and assign each customer a risk profile after identifying the importance and the appropriate weight of the overall risk for each evaluation element;
- equip themselves with tools to check the information relating to the customer, the person carrying out the transaction and the ultimate owner, which can be obtained from a reliable and independent source.

4.2 GUIDELINES

The Board of Directors encourages the Bank to follow these guidelines:

- Customer knowledge is crucial - Adequate customer verification and monitoring over time are critical steps in the implementation of anti-money laundering obligations. One of the main principles of the money laundering prevention and detection system is customer knowledge, right from the beginning of the business relationship (or the completion of single transactions);

- Verification must be adequate and confirmed – Customer knowledge must be "adequate". If it is lacking, then the bank will be exposed to legal sanctions. If excessive, it risks inefficiency, because too much control disperses resources which could be used better. The verification must make it possible to overcome any barriers that stand in the way of finding the final beneficiary of the transaction and the availability of amounts deposited and transferred. The information relating to the customer the person carrying out the transaction and the ultimate owner must be identified by a reliable and independent source;

- The verification process must be consistent throughout the Bank's organisational units – There must be consistency of conduct when carrying out adequate verification, between all organisational units. Over time, this will strengthen the controls within the Bank and make it possible to demonstrate to the relevant authorities that the specific measures taken are adequate for the identified risks;

- The depth and extent of the obligations are consistent with the customer profile - The adequate verification process aims to identify the depth and extent of the prevention and monitoring requirements by assigning a specific risk profile to

each customer based on the information acquired and the analyses carried out. The depth and extent of these requirements are defined beforehand by the Bank. This includes cases when it is necessary to verify the appropriateness of the assigned risk profile where there are events or circumstances that are likely to change it;

- IT procedures are helpful but do not replace the human factor - Structured procedures for collecting data and information through questionnaires, and the related support for processing the risk profile through predefined algorithms which can automatically assign the customer risk profile, are essential to ensure consistency and effectiveness of the adequate verification process. However, they cannot replace the prudent appreciation of a person who handles the adequate verification and monitoring during an ongoing relationship.

4.3 RISK CLASSES

Considering the Bank's current business model, customers were divided into three segments:

- Consumer families
- Producing families
- Companies

Based on this classification, the following risk classes for money laundering and international terrorism financing have been identified:

RISK LEVEL	DESCRIPTION
Irrelevant	A reduced risk level may be associated with subjects and products for which the simplified procedures for the adequate verification required by art. 25 of Legislative Decree 231/07 apply.
Low	A low risk level may be associated with subjects with limited assets and transactions.
Medium	A medium risk level may be associated with subjects operating in sectors exposed to a higher risk of money laundering or in geographic areas which have higher rates of illicit phenomena which could fuel money laundering activities. These sectors/ phenomena/areas are indicated in periodic reports such as those prepared by MEF, UIF - Bank of Italy, ABI-ARMA Interbank Committee, and Guardia di Finanza.
High	A high-risk level can be associated with subjects and operations where stronger obligations of adequate verification are required. Particularly:

	• operations which run exclusively at a distance, even during the initial phase of identification, and adequate verification of the subjects prior to the opening of the relationship; • politically exposed persons, including nationals, or other names present in watch lists; • relations with bodies of non-EU countries or with at risk countries and areas; • cash payment transactions, especially in large denomination banknotes, or cash from other countries above the threshold limits set by the regulations on currency monitoring; • use of products, transactions, technologies that can promote anonymity (e.g. tax shield operations, and interposition of trust mechanisms); • customers already subject to suspicious transaction reporting.

4.4 RISK PROFILE ASSIGNMENT

The Bank profiles customers in order to assign one of the previously mentioned risk classes by acquiring customer information, relationship details, and information connected to the transaction, as indicated below. This is carried out using a dedicated questionnaire and processing the related answers. (The reference IT procedures used for this purpose are provided by external outsourcers CEDACRI and OASI operating under specific contracts.)

Risk profiling is based on the combination of the following objective and subjective information:

- Personal details
- Legal nature
- Transactions
- Current accounts
- Cheques
- Financial instruments
- Channels (internet and telephone)
- Credit limits
- Geographic area
- Safety deposit boxes
- Prepaid cards
- Politically exposed person lists
- Terrorism lists
- Other lists
- Geographic area
- Reports of suspicious transactions

The Bank considers the following factors related to the customer as relevant:

- characteristics and legal nature of the customer (natural[1] or legal person[2]);

[1] Attributes of a "natural" customer:
- Known information about criminal proceedings or proceedings for tax damages and the imposition of administrative sanctions for violation of anti-money laundering provisions.

- Main activity[3];
- Behaviour[4];
- Geographic area of residence or location of the customer or counterparty[5].

The Bank considers the following factors related to the ongoing relationship/transaction as relevant:

- Type of transaction or ongoing relationship[6];
- Methods of carrying out the transaction or relationship[7];

- Information on subjects known to the customer (for example, family or business relationships);
- Holding an institutional, political, association, foundation or corporate office.

[2] Attributes of a "legal" customer:
- It is necessary to evaluate the corporate purpose, pursued objectives, operating methods, and legal form used;
- The connection between a legal person and entities resident in non-equivalent jurisdictions is relevant;
- Any situations of economic and financial difficulty or weakness which may expose them to the risk of criminal infiltration should be assessed;
- The characteristics of the person carrying out the transaction and the ultimate owner is essential, when the name is unknown to the recipient and not covered by any secrecy obligations that prevent it from being used by the recipient.

[3] Activity carried out and economic interests:
- Detects financial activities which can be traced back to those types of business which present money laundering risks (e.g. economic activities characterised by high financial flows movements or high use of cash) and require specific precautions;
- Detects transactions in those economic sectors affected by the provision of public funds, also from EU sources (for example, procurement, health, waste collection and disposal, renewable energy production);
- Detects the type of relationships and transactions, as factors to be considered when assessing the customer's business and economic interests.

[4] Detects any concealed actions when carrying out the transaction or establishing an ongoing relationship: the reluctance of a customer or of the person performing the transaction to provide the requested information; they incomplete or incorrect provision of information (such as identification information, ultimate owner identification, or information related to the transaction or relationship's nature and purpose).

[5] Customer and counterparty geographic area:
- Detects the residence or registered office and the business location;
- Detects illicit events which are likely to fuel money laundering in the area of activity: the degree of infiltration of economic crime, socio-economic or institutional weakness factors, "and the underground economy" phenomena. Attention should be paid when the area of interest is abroad. In this case, the risk elements inherent in the political-economic situation and the legal and institutional framework of the reference country are relevant.

[6] Detects the greater or lesser possibility of using the relationship or transaction for illicit purposes (e.g. cash transactions, credit transfers, especially if from or to non-EU countries other than equivalent third-party countries).

[7] Method of establishment and progress of the relationship or transaction:
- Lack of the customer's physical presence or direct identification (e.g. through the interposition of external partners);
- Transactions in cash and/or resources from or to foreign countries;

- Amount[8]/transaction frequency and relationship duration[9];
- The operation's or the ongoing relationship's reasonableness[10];
- Recipient's geographical area[11].

4.5 RISK PROFILE MONITORING FREQUENCY AND RELATED MEASURES

The monitoring activity assumes that the documents, data or information held about the customer, the ongoing relationship and the transactions are updated continuously.

The monitoring activity is conducted with the following frequency:

MONITORING FREQUENCY	SUBSEQUENT ACTIVITIES
Verification of the requisites' ongoing existence which made it possible to classify customers who are subject to simplified adequate verification (e.g. correct assignment of SAE and registration on the official register of the supervisory authority that issued the authorisation).	When that requirement is no longer met, the Bank provides a money laundering risk profiling questionnaire and classifies the customer into one of the other risk classes indicated above.
Monthly monitoring of the customer's operations through the "Gianos-Inattesi" application.	If the automated analysis of transactions shows that the customer has carried out transactions which are potentially incompatible with the acquired information, the Bank shall assess the submission of a suspicious transaction report.
Monitoring of customers in the irrelevant, low and medium risk categories is usually on a three-year basis.	Performance of the activities envisaged by Ordinary Adequate Verification.

- Transactions characterised by an unjustified level of complexity.

[8] Amount:
  Relationships related to the offer of private banking services for the customised management of a customer's substantial assets;
- Large transactions inconsistent with the customer's economic and financial profile;
- Use of high-denomination banknotes (Euro 500);
- Operations which elude anti-money laundering obligations.

[9] The frequency of transactions and duration of the ongoing relationship inconsistent with the economic and financial needs of the customer and the relationship's purpose and nature.

[10] Relationship/transaction reasonableness:
- Detects the customer's overall economic profile, based on all available information (e.g. need for financial services, income, and capital capacity);
- Comparative evaluations of the transactions of subjects with equivalent size, economic, or geographical characteristics are useful.

[11] Detects the geographic area receiving the funds or financial instruments which are involved in the ongoing relationship or transaction.

Monitoring of high-risk customers is usually on a six-monthly basis.	Performance of the activities envisaged by Reinforced Adequate Verification.

Regardless of the frequency of the checks planned by the Bank, events likely to change a risk profile are:

- Significant changes in customer operations[12];
- Substantial changes in the company structure;
- Acquisition of the "politically exposed person" qualification;
- Change of ultimate ownership.

The results of the monitoring activity can lead to:

- Updating of data, information and risk profiles;
- Carrying out more extensive and thorough checks (including the application of Reinforced Adequate Verification);
- Identification of anomalies and inconsistencies that may lead to suspicious transaction reporting;
- Asset-freezing, abstention from carrying out the transaction, or relationship termination.

4.6 DATA COLLECTION AND INFORMATION PROCESSING

The GIANOS system uses a structured data and information collection procedure which can automatically process and assign the risk profile of each customer and which checks the relationship progress over time.

GIANOS is divided into the following modules:

- "Kyc - Know Your Customer" enables completion of the electronic questionnaire to carry out adequate customer verification and to profile them when starting an ongoing relationship or executing an occasional transaction[13];
- "Risk Profiles" help manage activities aimed at monitoring the customer risk profile. The module determines the customer's risk score for money laundering or terrorism financing and assigns it within a range in which the customer can be classified for more or less incisive future checks;
- "Unexpected transaction evaluation" which is dedicated to the evaluation of transactions extracted through the batch procedure from the process generating anomaly indices for suspicious transactions;

12 The risk profile may be updated at any time if, by analysing the transactions completed, they are not fully compatible with the Bank's knowledge of the customer, its commercial activities and risk profile, and the fund's origin.

13 A specimen of the questionnaire and the weights assigned to each answer are reported in Part 3 of the Anti-Money Laundering Manual, devoted to adequate customer verification.

- Usury", as an aid to an effective identification of usury operations. The module generates "unexpected" files into the "Unexpected Transaction Evaluation" module referred to in the previous point;
- "Internal controls," aimed at checking the anomaly management processes, suspicious transaction reporting(SOS) phases, risk profiles and the centralised computer archive (AUI) records;
- "Diagnostic AUI", aimed at checking the records made in the Centralised Computer Archive and giving a formal and logical correctness analysis and a performance analysis using analytical causal factors to monitor potential omissions of AUI records.

4.7 INFORMATION FEEDBACK TOOLS

The main, reliable and independent feedback tools used to provide information on the customer, the person carrying out the transaction and the ultimate owner are the following:

- Unexpired identity documents needed by the Bank, other than those used during the adequate verification phase. Identification data for minors must be verified through the birth certificate or a court order, if any. For non-EU subjects, personal data must be verified through passport, residence permit or another equivalent document;
- Public deeds and authenticated private documents;
- A declaration of the Italian diplomatic mission and consular authority;
- Chamber of Commerce archives;
- Registers and lists of authorised subjects(e.g. financial intermediaries);
- Deeds of incorporation, articles of association, financial statements or equivalent documents, communications made public in compliance with sector regulations (such as statements, notices of significant shareholdings or privileged information), for legal entities;
- Information from public bodies and authorities, including the public administration of foreign states, provided that they are equivalent third-party countries;
- Information from public bodies and authorities acquired through websites (e.g. online services of the Revenue Agency for the verification of the tax code and VAT number);
- Paid database services (e.g. for searching names on watch lists).

5. ADEQUATE VERIFICATION AND DUTY TO ABSTAIN

5.1 LEGISLATIVE DECREE 231/07 AND RELEVANT IMPLEMENTING RULES

Article 23, paragraph 1 of Legislative Decree 231/07 insists that if the intermediary cannot comply with the customer adequate verification obligations, ongoing relationships or business operations should not be carried out, and any existing ongoing relationships should be terminated. The subsequent article 23, paragraph 1-bis, governs the procedure to be followed to return to the customer any available financial resources.

The relevant implementing rules require intermediaries to:

1. verify the details of the information gathered during an adequate verification;
2. establish the steps for its prompt integration in the absence of sufficient information;
3. terminate an ongoing relationship, when there is not enough information and return the customer's funds to another intermediary's current account;
4. send a message to the banking counterparty stating that the funds have been returned due to the impossibility of carrying out the adequate verification;
5. evaluate whether to send a suspicious transaction report.

5.2 GUIDELINES

The Board of Directors encourages the Bank to follow these guidelines:

- The duty to abstain prevents the establishment of an ongoing relationship - If it is impossible to go ahead with the adequate customer verification, the constitution of the ongoing relationship is prevented. Given the fungibility of money, a deposit of "dirty money" automatically implies its replacement (and therefore its laundering), as the Bank is obliged to return the same amount of money deposited to the depositor;

- The duty to abstain needs the customers to receive complete information about their duties regarding adequate verification - At the start of the relationship, the Bank reminds the customers of the consequences arising from the failure to complete the proper verification. The appropriately informed customers who refuse or are reluctant to give the requested information, provide false or counterfeit information, or repeatedly change the information provided without clear justification, violate their duties, and expose themselves to the risk of a suspicious transaction report;

- The return obligation needs full disclosure to the customer on the risks involved if there is non-cooperation - If the Bank learns that there is an absolute impossibility of carrying out or completing the adequate verification, it will promptly inform the customer, asking the details of an account on which to repay any available funds. The Bank shall explain the consequences of failure to carry out adequate checks, making specific reference to the obligation to send a message to the banking counterparty stating the repayment reasons, or - if there is a failure to give such details - stating the requirement to transfer the sums to a non-interest-bearing account. The diligence of the Bank mitigates the risk of disputes and litigation.

6. ACTIVE COOPERATION

6.1 LEGISLATIVE DECREE 231/07 AND RELEVANT IMPLEMENTING RULES

Article 41, paragraph 1 of Legislative Decree 231/07 imposes an obligation on intermediaries to report suspicious transactions to the Financial Intelligence Unit (UIF) when they know, suspect or have reasonable grounds to suspect that money laundering or terrorism financing operations have been carried out or attempted.

Intermediaries are required:

- to deduce the suspicion from the characteristics, extent, nature of the transaction or any other known circumstance;
- to consider the economic capacity and the activity carried out by the subject to whom the report refers, based on the elements available and information acquired during the process.

6.2 GUIDELINES

The Board of Directors encourages the Bank to follow these guidelines:

- Active collaboration is at the heart of the prevention system - Suspicious transaction reporting is mandatory when the Bank knows, suspects, or has reasonable grounds to suspect that money laundering or terrorism financing operations are being carried out or attempted. Maximum confidentiality must be ensured in the reporting process to protect the reporting subject;

- Only the quality of the reporting provides an effective contribution to the fight against money laundering - The bank's activities must be guided by sensitivity, weighting, and the ability to discern anomalies inherent in a transaction. The reporting must originate from a qualified suspicion, and be the result of an incisive selection filter. The reporting obligation does not require certainty about the criminal origin of the sums, as a reasonable doubt is sufficient;

- Anomaly indicators and systems showing unusual behaviour reduce uncertainty margins - The analysis of transactions for reporting purposes is carried out for the entire duration of the relationship and cannot be limited to the establishment or termination phases. The indicators provided by the supervisory authorities are of considerable help in this process even if the occurrence of such behaviour is an insufficient reason for reporting, while the absence of indicators is not enough to rule out suspicious transactions;

- Traceability of cash flows helps the identification of suspicious transactions - A widespread channelling of financial flows to the Bank, and correct and timely input of the Centralised Computer Archive, allow an extensive use of data and information relating to the customer, the ongoing relationship and the transaction, and aid the identification of suspicious transactions.

7. RELATED DOCUMENTS

No.	*Document Type*	*Document title*
1	Manual (Anti-Money Laundering)	Part 1 - Legal Framework
2	Manual (Anti-Money Laundering)	Part 2 - Organisational Model
3	Manual (Anti-Money Laundering)	Part 3 - Adequate verification of customers
4	Manual (Anti-Money Laundering)	Part 4 - Document Storage, AUI and SARA
5	Manual (Anti-Money Laundering)	Part 5 - Reporting of suspicious transactions
6	Manual (Anti-Money Laundering)	Part 6 - Limitations of cash and bearer securities