ICBC (EUROPE) S.A.
MILAN BRANCH

ORGANISATIONAL, MANAGEMENT AND CONTROL MODEL

pursuant to Legislative Decree no. 231/2001

Approved by the Board of Directors of ICBC (Europe) S.A. on 18 June 2019 -

(Lastly updated in 2024)

Definitions

The terms used in this document have the following meanings. Words denoting the singular number shall include the plural and vice versa.

- **"Association":** entities/bodies composed of two or more persons in order to achieve well-defined objectives, generally altruistic or ideal, or to provide an advantage for the associates.
- "**Authorities of Public Security**" any authority (international and US too) entitled with powers on public security and/or surveillance, including the authority and powers to issue restrictive measures to the individuals and entities listed as per terrorism financing and any other restrictive financial measure;
- **"Board of Directors":** the Board of Directors of ICBC (Europe) S.A., having its registered office in Luxembourg, and its members;
- "**Branch**": is the Branch that ICBC (Europe) S.A. opened in 2, Tommaso Grossi Street, Milan, including its local unit in Rome, Via Muzio Clementi 74;
- "**CCNL**": the relevant National Collective Labour Agreement in force from time to time, signed at Italian national level, between organizations representing employees and their employers;
- **"Code of Conduct":** the policy issued by Headquarter and adopted by the Branch, outlining obligations for the employees to comply with principles, policies and laws outlined in that policy;
- "**Code of Ethics**": the policy adopted by the Branch, indicating a set of behavioral rules that all Recipients must respect in order to prevent situations that could compromise the integrity of the Branch;
- "**Committees**": collegial bodies that the Branch set up within the organization and that are in charge in order to treat and discuss regarding specific matters;
- **"Company**": a group of individuals endowed with different levels of autonomy, relationship and organization that, in various combinations, interact in order to pursue one or more common objectives;
- **"Consob":** the National Commission for Companies and Stock Exchange is a public authority responsible for regulating the Italian securities market and protecting the investing public.
- "**Consultant**": a person who professionally provides expert advices by a mandate contract or other contractual relationship;
- "**Department":** organisational units in which the Branch is divided in relation to the different powers and duties;
- **"Entity":** legal persons, Companies and Associations, including those without legal personality;
- **"External Parties":** self-employed, "para-subordinate workers", freelance professionals, consultants, agents, outsourcers, commercial partners, etc. not belonging to the Branch that collaborate with the Branch;

- **“Families of crime”:** set of crimes provided for by the Legislative Decree no. 231/01 as Predicate offences for the potential configuration of the Entity’s administrative liability;
- **“Finance Intelligence Unit”**: a specialized unit, within the Bank of Italy, in charge for examining financial flows, acquiring information and receiving reports of suspicious transactions by obliged parties, carrying out a financial analysis of the information and evaluating whether to transmit them to the investigative bodies, collaborating with the judicial authority for any repression;
- **“Guidelines”:** Guidelines of the Italian Banking Association (“ABI”), Association of Foreign Banks in Italy (“AIBE”) and Confindustria for the drafting of Organisational, Management and Control Models for banking sector pursuant to Legislative Decree no. 231/01, as subsequently integrated and modified;
- “**Headquarter**”: ICBC (Europe) S.A., having its registered office in Luxembourg, at 32, Boulevard Royal, L-2449;
- **“Risk Assessment”:** a map in order to identify and analyse the Branch's exposure to the risks related to the application of the Decree, indicating the activities at risk carried out by each Department, the predicate offences that could be committed in the context of such activities, the relevant safeguards adopted by the Branch and the related internal regulations.
- “**Non-Manager Employees**”: all employees of the Branch (other than Senior **positions/** Senior Persons) that are under the management and/or supervision of a Senior Person;
- **“Organisational, Management and Control Model” or “Model”**: is the organizational model drawn up and adopted by the Branch in compliance with the provisions of Legislative Decree no. 231/2001 aimed at preventing administrative liabilities of the Branch;
- **“Head Office”:** “Industrial and Commercial Bank of China Limited”, based in Beijing, People's Republic of China;
- “**Predicate crimes/offences**”: crimes which, if committed, may result in the administrative liability of the Branch in accordance with the Legislative Decree no. 231/01;
- **“Public Administration”:** the Italian Public Administration and, with specific reference to offences against the Public Administration, Public Officials and persons in charge of a public services;
- **“Recipients”:** all employees of the Branch and External Parties who collaborate with the Branch;
- **“Regulation”:** means the regulation governing the scope, the composition of, and the procedure to be followed by, the Surveillance Body;
- **“Risky Activities”:** activities of the Branch that are considered at risk of commission of the Predicate offences pursuant to the Legislative Decree no. 231/01, as identified under the column “Sensitive Macro Area” in the Risk Assessment of the Branch;
- **“Senior positions/ Senior persons”:** people holding representation, administration or management functions of the entity or by one of its organizational units endowed with financial and functional autonomy and by people performing the *de facto* management or control thereof.

For the Branch, “Senior positions/ senior persons” are meant to be the General Management;

- **“Staff Handbook**”: the Manual addressed by the Branch to its employees, in order to describe the expectation that the Branch has towards its employees and to outline the policies, programs and benefit available;
- “**Surveillance Body**”: an independent Body that is in charge to supervise on correctness, effectiveness and applicability and continuous updating of the Model;
- “**Tax Authority**” or “**Financial Authority**” the local tax Authority receiving by the Branch tax declarations and/or the mandatory reporting provided by law and regulation that can require (acting through the tax police too) the data acquiring and/or documentation;
- **“Third Parties”:** all parties different from the Branch and the External Parties that may be indirectly involved but is not a principal party to an arrangement, contract, deal, lawsuit, or transaction.

Acronyms

- **“AML/CTF”**: Anti-Money Laundering and Counter Terrorism Financing
- “**CIB”:** Corporate & Investment Banking Department
- “**CONSOB**”: National Commission for Companies and Stock Exchange
- “**DPO**”: Data Protection Officer
- **“ESG”**: Environmental Social Governance
- “**FI**”: Financial Institutions Department
- **“GAD”**: General Administration Department
- **“GM”:** General Management
- **“HQ”:** Headquarter
- “**ICBC”**: Industrial and Commercial Bank of China
- **“INAIL”**: National Institute for Insurance against Accidents at Work
- **“INPS”**: Italian National Social Security Institution
- **“IT”:** Information Technology
- **“KYC**: Know Your Customer
- **“MLRO”**: Money Laundering Reporting Officer
- **“UIF”**: Financial Intelligence Unit

GENERAL PART

CHAPTER 1 - THE REGULATORY FRAMEWORK

1.1. Introduction

The Legislative Decree no. 231 of 8 June 2001 (hereinafter the “Decree” or “Legislative Decree no. 231/01”) introduced for the first time into the Italian legal system the administrative liability of legal entities, companies and associations, including those without legal personality for administrative offences arising from a crime. According to the rules introduced by the Decree, entities can be held “liable” in relation to certain crimes actually committed or attempted, where they have been carried out in the interest of or to the advantage of the Entity itself by senior officers of the Company and by those who are subject to their management or supervision and where the entity failed to adopt adequate preventive measures capable of preventing the commission of the offences by the mentioned subjects.

The entity’s liability may exist even if the alleged offence is configured as a crime of attempt, meaning thereby when the subject commits acts unequivocally directed to committing a crime and the action is not committed or the event does not occur.

The entity’s administrative liability is entitled to be liable for any crime (s.c. Predicated Offences) committed abroad even if it is a Branch (both UE and/or not UE).

The administrative liability of entities is to be considered further and independent from the criminal liability recognized at the individuals who have committed the crime despite the fact that the Entity's administrative liability is normally established in the same criminal proceedings brought against the natural person. However, the entity’s liability persists also in case the natural person who committed the crime is not defined or is found to be not punishable.

Moreover, the Decree has introduced new provisions with reference to the sanctioning profile, in fact, Entities are subject to sanctions of both a pecuniary and interdictory nature as a consequence of the commission of offences by persons connected to it.

Concerning the effectiveness and enforceability of the Model, a material evaluation on the 231 sanctions applied on conducts representing infringements of the rules provided by the Model is also provided.

1.2. Perpetrators of the Predicated Offence(s)

According to Article 5 of the Decree, an Entity is responsible for crimes committed or attempted in its interest or to its advantage:

- by “persons who occupy positions to represent, administer or manage an Entity or one of its organisational units which are financially and functionally autonomous and also by persons who also de facto manage and control the Entity itself” (the persons defined above as being in a “Senior position” or “Senior” persons, Art 5, paragraph 1, letter a) of Legislative Decree no. 231/01; or

- by persons subject to the management or supervision of one of the senior persons (the persons defined above as being in a “Non-Manager” position” as being subject to the management or supervision of others; Art 5, paragraph 1, letter b) of Legislative Decree no. 231/01).

The crimes are defined as committed in the interest of and to the advantage of an Entity when the Entity has received, or in any case could theoretically receive, any positive return whatsoever in relation to the commission of the offence in both financial terms or in terms of another nature, inclusive therein of savings made on resources. It must also be stated that, by express provision of the law (Article 5, paragraph 2 of Legislative Decree no. 231/01), an Entity is not liable if the persons listed above acted solely in their own interests or those of Third parties.

1.3. The Predicate offences for corporate liability

Crimes for which an Entity may be held responsible according to the Decree (if committed in the interest of or to the advantage of persons specified under Article 5, paragraph 1 of the Decree) can be classified in the following categories:

1. Offences against the Public Administration, extortion, unduly inducing to give or promise ad advantage and corruption (referred to in article 24 and 25 of the Decree);
2. Computer crimes and unlawful data processing (referred to in article 24-bis of Decree);
3. Organized crime offences (referred to in article 24-ter of the Decree);
4. Offences concerning the counterfeiting of money and valuables (referred to in article 25-bis of the Decree);
5. Crimes against industry and trade (referred to in article 25-bis.1 of the Decree);
6. Corporate offences (referred to in Article 25-ter of the Decree);
7. Crimes for the purposes of terrorism or subversion of the democratic order (referred to in article 25-quater of the Decree);
8. Crimes against female genital mutilation practices (referred to in article 25-quater.1 of the Decree);
9. Crimes against individuals (mentioned in article 25-quinquies of the Decree);
10. Market abuse (referred to in Article 25-sexies of the Decree 231 and article 187-quinquies of the Consolidated Finance Law);
11. Workplace health and safety offences (referred to in article 25-septies of the Decree);
12. Crimes concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering (referred to in article 25-octies of the Decree);
13. Offences relating to non-cash payment instruments (Art. 25-octies.1 of the Decree);
14. Crimes involving breach of copyright (referred to in article 25-novies of the Decree);
15. The crime of “Inducement not to make or to make false statements to judicial authorities” (referred to in article 25-decies of the Decree);
16. Offences against the environment (referred to in article 25-undecies of the Decree);

17. Crimes of employment of third-country citizens whose stay is irregular (referred to in article 25-duodecies of the Decree);

18. Crimes of racism and xenophobia (referred to in Article 25-terdecies of the Decree);

19. Fraud in sporting competitions, illegal practice in gambling sector and through banned means (referred to in article 25-quaterdecies);

20. Tax Predicated Offence (referred to in article 25-quinquiesdecies);

21. Smuggling (referred to in art. 25-sexiesdecies);

22. Crimes against cultural heritage (Article 25-septiesdecies of the Decree);

23. Laundering of cultural assets and devastation and looting of cultural and landscape assets (Art. 25-duodicies of the Decree);

24. Transnational offences (referred to in Article 10 of Law No. 146 of 16th March 2006 which "ratifies and implements the United Nations convention and protocols on transnational organised crime, adopted by the General Assembly on 15th November 2000 and 31st May 2001");

25. Counterfeiting and / or sanitary adulteration (Law No. 9/2013 art. 12)

26. Fraud against the European Agricultural Fund (L. No. 898/1986, Article 2).

1.4. Penalties

The following penalties are provided by the Legislative Decree no. 231/01 for Entities, as a consequence of committing or attempting to commit the aforementioned crimes by Senior Person or a Non-Manager Employee:

1) Interdiction sanctions: Penalties of a prohibition nature (applicable even as a "precautionary measure[1]") of a duration of not less than three months and not more than two years, which may consist of:
   - disqualification from carrying on a business;
   - suspension or revocation of authorizations, licenses or concessions relating to the offence committed;
   - disqualification from contracting with the Public Administration, except for obtaining the service of a public agency;
   - exclusion from entitlement to public concessions, grants, contribution or subsidies and the revocation of those already granted;
   - prohibition on advertising goods or services;
2) confiscation of profits of the crime;
3) publication of the judgment;

[1] And therefore before investigating into the merit of the existence of an administrative crime or misconduct that arise from it, in case serious evidence is found leading to retain the entity liable, as well as in the case of the danger that the offence could be reiterated. In the case in which a judge finds the existence of grounds for the application of interdictory sanctions to an entity performing activities of public interest or that has a sizable number of employees, the judge will be able to decide that the entity continue to operate under a judicial commissioner.

4) financial penalties

Fines are decided by the criminal Judge by using a system based on “quotas”, which are not less than one hundred and not greater than one thousand in number and which are variable in amount for each single “quota”, varying from a minimum of €258.23 to a maximum of €1,549.37 (and therefore for an amount which ranges from a minimum of €25,823.00 and a maximum of €1,549,370.00).

As said, an Entity is deemed liable even in cases of attempted crimes, which is configured in cases where actions have been carried out and designed unequivocally to commit one of the crimes which constitute Predicate offences by the Entity. In these cases, fines (in terms of amount) and prohibition penalties (in terms of time) are reduced between one third and one half, while no penalties are imposed in cases in which the Entity voluntarily prevents the act from being accomplished or the event from occurring (Article 26 of the Decree).

1.5. Exemption from administrative liability

Having established the administrative liability of entities, Article 6 of the Decree establishes that the Entity shall not be liable if it can prove that:

a) the Entity had adopted and effectively implemented an appropriate organizational and management model to prevent offences of the kind that has occurred;
b) the task of monitoring the Model implementation, compliance and updating was entrusted to a corporate body with independent powers of initiative and control;
c) the perpetrators committed the offence by fraudulently circumventing the Model;
d) there was no omission or insufficient control by the control body.

Moreover, where the offence is committed by Non-Manager Employees, the Entity is liable if perpetration of the offence was made possible by non-performance of management and supervisory duties. Such non-performance shall be ruled out where the Entity, before the offence was committed, had adopted and effectively implemented an appropriate Model to prevent offences of the kind committed, based, of course, on an a priori assessment.

1.6 Crimes committed abroad

In accordance with Article 4 of the Decree, an Entity may be held liable in Italy for the commission of Predicated crimes that are committed abroad. The illustrative report on the Decree underlines the need to avoid a type of criminal situation, which frequently occurs, from going unpunished and also to prevent the entire legislation in question from being easily evaded.

1.7 Contents of the Models

Article 6 of the Decree provides that the Model must:

- identify the activities which may give rise to the offences listed in the Decree;
- provide for specific protocols aimed at planning the formation and implementation of the

Entity's decisions in relation to the offences to be prevented; define procedures for managing financial resources to prevent offences from being committed;

- establish reporting obligations to the body responsible for monitoring the Model's operation and compliance;
- put in place an effective disciplinary system to punish non-compliance with measures required by the Model.

This Model was drafted and updated also having regard to the Guidelines. Any misalignments of any provision of this Model from the principles set out in the Guidelines has been evaluated and assessed having regard to, among others, the actual organization of the Branch and the Headquarter and the relevant Italian market practice.

CHAPTER 2 - THE ORGANISATIONAL STRUCTURE AND CORPORATE OPERATION OF THE BRANCH

2.1. The Branch

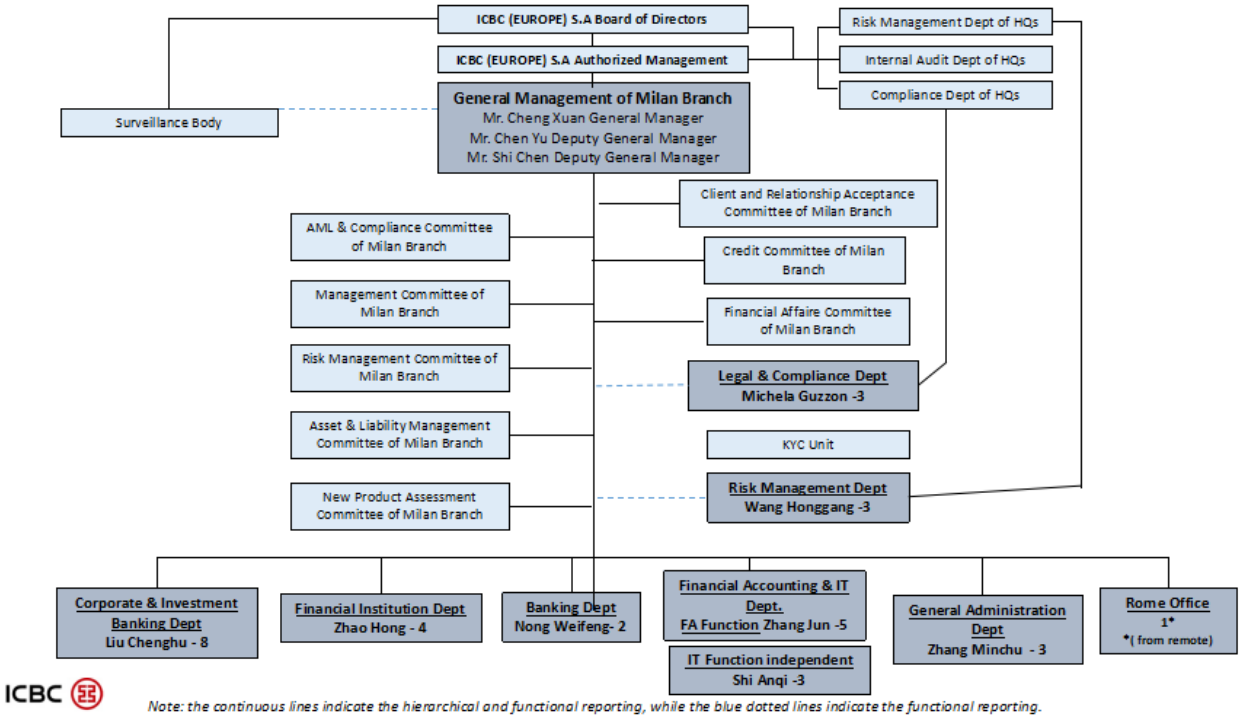
ICBC (Europe) S.A., Milan Branch is located in Italy since 18 January 2011 with the office at 2, Via Tommaso Grossi in Milan, registered in the "Companies Register of Milan" under the no. 07132530960. In 2015 the Branch also opened local unit in Rome.

The Headquarter is located in Luxembourg and having its registered office at 32, Boulevard Royal, L-2449 Luxemburg and it is registered in the "Registre de Commerce et des Sociétés Luxemburg" under the no. B 119320.

The Head Office is based in Beijing, People's Republic of China.

The organizational and operational structure of the Branch should be clear, transparent, consistent, complete and free from conflicts of interest, as evidenced by the following Organizational Chart[2] as of June 2024:

[2] In the following Organisational Chart of the Branch solid lines indicate the functional and hierarchical reporting, while the dotted lines in blue indicate the functional reporting. In particular, from a hierarchical and functional point of view, the Internal Control Functions of the Branch (Legal & Compliance and Risk Management Departments, marked in red color) have hierarchical and functional link to the internal control functions of the Headquarter in Luxembourg.



The General Management is responsible for the management of the Branch and is composed of the General Manager (also legal representative of the Branch) and two Deputy General Managers (together, the "**General Management**"). The General Management has the overall responsibility for the Branch.

The General Management shall ensure the execution of activities and preserve business continuity, by way of example administration, internal governance arrangements and the business strategy of the Branch. The General Management receives decision powers by delegation from the Headquarter on an annual basis, commits itself to act within guiding principles and authorizations granted by the Headquarter.

The members of the General Management, who are potentially subjected to a conflict of interest, shall promptly inform the other members of the General Management on their own initiative shall abstain from participating in the decision-making processes where they may have a conflict of interest or which prevent them from deciding with full objectivity and independence.

The Organizational Chart shows the relative structure and functional and hierarchical reporting with General Management and the Headquarter.

2.2. The main area of operation of the Branch

The priority of the Branch is to offer services to promote economic and trade exchanges between China and Italy. The Branch carries out banking, trading and investment banking activities, offering clients services such as time deposits, financing, payment services, issuing of guarantees and trade finance. The Branch also makes investments in bonds and carries out money market and foreign exchange transactions exclusively on its own proprietary portfolio (i.e. not on behalf of clients); to a

residual extent, spot foreign exchange transactions are carried out with clients.
In terms of target customers, given the current market conditions, the limited risk propensity and the international nature of ICBC Group, the Branch decided to focus on the following targets:

- companies among the Fortune 500 and Italian companies among the top 50 listed;
- companies with strong internationalization and with high external rating;
- companies with stable and satisfactory cash flow;
- primary Chinese companies investing overseas;
- Italian banks and Financial Institutions.

Despite being authorized to do so, the Branch does not provide financial or investment services falling under Mifid II regulations to its customers.
In addition, the Branch coordinates the activities of the Rome Office, focused on the commercial development and on the relationship management with customers in central and southern Italy.

2.3. The corporate governance of the Branch

The Branch has an organisational and governance structure that includes Committees (see paragraph 2.3.2 below for details), internal control bodies (see paragraph 2.3.3 below for details) and internal control reporting systems (see paragraph 2.3.4 below for details) in line with local legislation and regulations, the requirements expressed by Bank of Italy, as well as the provisions of the policies and procedures provided from the Headquarter, reflecting the requirements of the Luxembourgish regulation, in compliance with the so-called “stricter rules” principle.

2.3.1. Responsibilities of Departments

There are three types of Departments in the Organizational Chart:

- Business units: including Corporate & Investment Banking Department, Financial Institution Department and the Rome Office, which are responsible for marketing and business operations;
- Supporting units: including the Banking Department, the General Administration Department and the Financial Accounting & IT Department;
- Internal control units: including the Legal & Compliance Department and the Risk Management Department. Internal Audit tasks are performed directly by the Internal Audit Department of the Headquarter.

Each Department of the Branch has its “operational mechanism” which includes the Department responsibility, staffing and relationship with other Departments and the General Management.

General Administration Department leads the management of human resources and the general administration of the Branch. The functioning of the Department includes staff management, recruiting, developing, training and, in general, to deal with various issues related to human resources management. In addition, it is in charge of strategic management and research work, publicity, security and archives management.

Banking Department is in charge of the operation of banking business. In particular, it is responsible for the customer account management, executing remittance, deposit and loan operation, correspondent banking clearing business, international settlement and trade finance business operation, including import and export letter of credit, inward/outward collection, guarantee. In addition, it is also responsible for the management of the settlement of funds not withdrawn from retail customers on the occasion of the closure of the retail business and still held at the Branch and the Treasury Back Office function.

Financial Accounting & IT Department is in charge for financial accounting & IT management of the Branch. The main responsibilities of this Department include organizing, controlling and performing the accounting treatment of the Branch, completing the accounting reports required locally, by the Headquarter and by the Head Office accurately and efficiently, managing the financial budget and annual assessment, asset and liability evaluation and management, assisting the external auditor in completing the relevant annual audit, handling local tax affairs of the Branch.

IT function (part of the Financial Accounting & IT Department) is in charge for information technology management of the Branch. In particular, it is responsible for the maintenance of production system to ensure its high availability, network and information security management, system requirement management, testing support and data governance.

Risk Management Department is a second-level control function responsible for identifying, managing and monitoring the overall risks within the Branch, including credit, market, liquidity and operational risk, by taking the lead to implement the risk management policies, requirements, risk appetites and limits stipulated by the Headquarter with the coordination of related departments; conducting examination on credit proposals and assisting the General Management in formulating local risk management policies and providing risk management recommendations.

Legal & Compliance Department is an internal control function involved at second level controls (as defined in compliance with the CSSF's Circulars – as general requirements - and by Supervisory provisions for banks Circular no. 285 of December 17, 2013 of the Bank of Italy - as local requirements -, all as time by time amended). It is an independent Function intended to supervise the non-conformity risks and the effective executions of the mandatory actions and controls on legal, compliance, anti-money laundering and counter terrorism financing.
The department provides operational guidance to support the Branch in the correct execution of controls and reviews in accordance with the applicable Italian and Luxembourgish regulations and the group policies. Main activities include: (i) control and monitoring of all measures taken to mitigate the compliance risks; (ii) conduct transaction monitoring and local regulatory reporting (AUI/SARA);

(iii) through the delegated Money Laundering Reporting Officer (i.e., the Head of the Department), escalation of suspicious cases to FIU.
In addition, responsibilities of the Legal function include taking charge of legal issues at the Branch level, support business development with other business Departments, manage legal disputes and prevent or deal with (potential) lawsuit.

Corporate and Investment Banking Department is responsible for the development of corporate and investment banking activities and customer relationships to promote the Branch's image to the Italian market. These tasks are carried out through the promotion of approved products and services to qualified customer, especially main corporate customers like granting a loan or in participating in syndicated loans (including revolving credit facilities and term loan) with Third-party banks.

Financial Institution Department leads the management of Financial Institution and Financial Markets business of the Branch. In particular, the department is mainly responsible for establishing and maintaining the business relationship with Financial Institutions, monitoring and managing Financial Institution counterparties and promoting the credit business of Financial Institutions. In addition, the department also has the duty to develop the Financial Market related business for the Branch.

Internal Audit is a function carried out directly by a division of the Headquarter on the basis of independent audit planning
Rome Office is responsible for managing the market development in Rome and the south part of Italy, analyzing market trends and participating in market activities.

2.3.2 Committees

In order to support the General Management in the exercise of its responsibility, Committees have been established in the Branch and they report to/inform directly the General Management. In particular, each Committee has a specific regulation that indicates the purposes, responsibilities, duties, memberships, meetings, organization procedures and reporting procedures.
A brief description of the Committees is provided below.
The Management Committee is composed of the General Management and the Heads and Deputy Heads of each Department. The Management Committee takes place once a month is and is in charge to monitor and discuss the Branch's strategy and other relevant issues concerning the Branch.

The Risk Management Committee is responsible for establishing and supervising risk management processes, defining the control model for credit risk, market risk, operational risk and liquidity risk, etc.

In addition, the Committee is responsible for the approval of internal regulations, and all issues related to risk management in general. The Committee is composed of the General Manager, the Heads and Deputy Heads of each Department.

The Credit Committee is composed of the Deputy General Managers, the Heads and Deputy Heads of Risk Management Department, Corporate & Investment Banking Department, Financial Institutions Department, Financial Accounting & IT Department, Banking Department and Legal & Compliance Department and it has the functions of supervising the implementation of credit policies and procedures, approving credit lines granted to customers, non-performing positions and the classification of loans. In addition, the Processor is responsible for recommending provisions on non-performing loans, litigation and write-offs and all relevant credit-related issues. The Head of the Legal and Compliance Department attends Committee meetings as non-voting legal and compliance experts

The Client Relationship Acceptance Committee ("CRAC") is composed of the General Manager (as Chairman of the Committee), the Deputy General Managers, the Head of the business Department who is presenting the prospect, the representative of Department (relationship manager) in charge of the prospect, the Head of Legal and Compliance Department and the Head of Risk Management Department or his back-up.

The CRAC has the overall responsibility for analysing the possible acceptance of high-risk customers (including corporate and financial institution or assimilated customers), as well as the continuation of existing relationships, when, following a periodic or event-driven review, the risk profile classification has been upgraded to high money laundering risk, also taking into account the sanctions and reputational profile.

The CRAC also assumes the task of monitoring on an ongoing basis the limits defined in the AML Risk Appetite Framework, ensuring that decisions made in relation to the opening of new client or other business relationships as well as the retention of existing clients are in line with the Branch's AML Risk Appetite.

The Anti-Money Laundering & Compliance Committee (AML and Compliance Committee) is responsible for supervising compliance with relevant internal regulations issued by Headquarter and external rules and regulations. The Committee is composed of the General Management, Deputy General Managers, Head of the Legal and Compliance Department, Head of the Risk Management Department and their Deputy Heads.

A brief description of the Credit Committee, the Client Relationship Acceptance Committee, the Finance Committee, the Asset and Liability Management Committee and the New Products Committee is given, in view of the active role they play in the management of the risks borne by the

Branch.

The Financial Affairs Committee is composed of the Deputy General Manager in charge for financial accounting and the Heads and/or Deputy Heads of the Financial Accounting & IT Department, General Administration, Banking, Financial Institution, Risk Management, Corporate & Investment Banking and Legal & Compliance Department. The Committee oversees the branch's financial management by analysing and monitoring internal and regulatory financial operating limits.

The Asset & Liability Management Committee is in charge of the discussion and analysis of every question relating to the asset and liability management and it is composed of the General Management and the Heads of the Risk Management, Financial Accounting & IT, Corporate & Investment Banking and Financial Institution Departments.

The New Product Assessment Committee is in charge of the discussion and approval of each new business product of the Branch, reviews the main aspects related to the approval of new products, including the adequacy of internal policies and procedures, the effectiveness of risk control measures, the necessary IT resources, etc. The Committee is composed of Deputy General Managers and the Heads and/or Deputy Heads of the Risk Management, Legal and Compliance, Financial Accounting and IT, Banking, Corporate and Investment Banking and Financial Institution Departments.

Finally, it should be noted that in June 2019, the Board of Directors of the Headquarter approved the establishment of the Surveillance Body.

Furthermore, the Branch may be invited and has access, if deemed necessary, to the Audit and Compliance Committee established by the Board of Directors of the Headquarter. The purpose of the Committee is to provide the Board of Directors with critical assessments in relation to the organisation and operations of the Bank. The Committee's scope of activity includes, among others, compliance and anti-money laundering and terrorism financing issues. The composition of this Committee is determined by the Board of Directors and includes at least three non-executive members of the Board of Directors who are not members of the Headquarter’s Authorised Management and who are not part of the Bank's staff.

2.3.3 The internal control system

The internal control functions of the Branch are carried out by Legal & Compliance Department and Risk Management Department.

In particular, the Legal & Compliance Department provides the Headquarter with a monthly report, detailing information on the activities carried out during the reference month, and an annual report

(Annual Compliance Report). In addition, further reports are submitted to the Headquarter upon request or for the purpose of conducting specific assessments included in the Compliance Monitoring Program, defined by Headquarter and implemented locally, which defines the objectives and periodicity of planned control activities on the basis of an annual Compliance Risk Assessment.
The Risk Management Department informs the Headquarter regularly on the status of the implementation of risk limits, credit asset quality, market risk exposure, operational risk indicators, etc., on a daily, weekly or monthly basis, as required, and sends overall risk management reports on a quarterly basis.
The Risk Management Department of the Branch coordinates with the Internal Audit Department of the Headquarter and the relevant functions of the Branch to ensure that the necessary measures are taken in a timely manner to remedy the deficiencies found during the audit.
The internal audit function is generally performed once a year by the Internal Audit Department of the Headquarter and covers all activities managed by the Branch.

The findings of the audit activities and related operational guidance are documented in reports addressed to the General Management of the Headquarter and the General Management of the Branch. These reports also provide a description of the corrective actions aimed at resolving and/or preventing the critical issues found. The reports are submitted to the Audit & Compliance Committee of ICBC (Europe) S.A.

2.3.4 Reporting of Internal Control Function

Internal Control Function (hereinafter, the “Branch ICF”) are represented by the Risk Management Department and the Legal & Compliance Department of the Branch that depend, from a hierarchical and functional point of view, on the internal control functions of the Headquarter (hereinafter, the “Headquarter ICF”), to which they report.
For reports to be sent to Supervisory Authorities the Branch should always submit in advance the relevant materials/documents to its General Management for review and final determination, assuming that the Branch shall comply with local applicable regulation.

2.4 The Organisational, Management and Control Model of the Branch: structure and summary

In order to prepare the Model, analysis have been carried out with a specific focus on the Activities at risk of potential commission of the predicate offences and the related mitigation and prevention measures adopted by the Branch.
The outcome of this activity constitutes the content of the individual sections of the Special Part of the Model, each one reporting - in relation to the families of crime examined - the risk activities involved and the respective measures and internal procedures of the Branch.
The activities considered relevant for the drafting and subsequent updating of the Model are those

which, following a specific risk assessment activity, have manifested risk factors relating to the commission of violations of the criminal provisions set out in Legislative Decree no. 231/01 or in the Branch's Code of Ethics and Code of Conduct.
A brief description of the phases in which the identification of Activities at risk was carried out, on the basis of which this Model was then prepared and updated, is given below.

Preliminary phase

The preliminary phase was aimed at acquiring the supporting documentation and planning the identification activities. Punctual analyses were carried out on the documentation in use at the Branch (organisational charts, risk and control surveys and assessment, operating procedures), and comparisons were made with the corporate Functions and Departments concerned, through targeted interviews in order to identify the top management to be involved in the subsequent risk assessment and control system phase.

Risk Assessment:

- execution of a risk mapping ("Risk Assessment"), in order to identify and analyse the exposure of the Branch to the risks connected to the application of the Decree, in which are indicated the Activities at risk carried out by each Department, the predicate offences that could be committed in the context of such activities, the relevant main safeguards adopted by the Branch and the reference internal procedures.
- sharing of the “Risk Assessment” with the Head of Legal & Compliance Department of the Branch in order to collect specific feedbacks on the correctness of the description of the risk activities and main safeguards identified;
- evaluation of feedbacks received on the “Risk Assessment”: This step allowed to improve the description of the preventive measures adopted by the Branch and to identify the relevant gaps.

Gap Analysis:

On the basis of the risk assessment activities and the current situation of the Branch and the preventive measures already in place, some gaps have been identified and additional preventive measures should be adopted, as required under applicable regulation.

Drafting of the Model:

This Model consists of a "General Part" and a "Special Part", divided into individual sections (“Sections of the Special Part”), drawn up for the different families of crime contemplated in the Decree. The General Part contains the general rules and principles of the Model, while the individual Sections of the Special Part identify the activities at risk of commission of the Predicate offences laid

down by the Decree.

2.5 The procedure to adopt the Model and its subsequent update

Despite the Italian Legislation provides the adoption of the Organizational, Management and Control Model as not mandatory, the Branch established to adopt the Model and, pursuant to a resolution of the Board of Directors of Headquarter, a Surveillance Body was established at the Branch, equipped with the related powers and the budget in order to carry out the activities within its competence.

In choosing to adopt its own Model, the Branch has taken into account the following elements:

- the possible consequences that the lack of adoption of a proper Model could have on the entity in the event of its involvement in proceedings for administrative liability for crime (fines, prohibitory sanctions, effects on image, credibility, etc.);
- the fact that the adoption of the Organisation and Management Model represents an essential requirement for entities operating in Italy, if not also a real obligation, so much so that even the legislator has taken such a course of action;
- the activity carried out by the Branch as an entity operating in the banking sector.

The Model is aimed at reflecting business operations, it must be adapted to the continuous evolution of the Branch's organization and the applicable legislative framework. The Board of Directors of Headquarter will deliberate on the subsequent amendments and integrations to carry out on the Model, upon the proposal made by the Surveillance Body.

By way of example, changes to the Model might be:

- inclusion in the Model of other Sections of Special Part relating to different types of offences which, due to other regulations, will be inserted in the future or, in any case, connected to the scope of the Decree;
- deletion of some Sections of Special Part of the Model;
- updating the Model following the significant reorganization of the Branch structure and / or of the overall corporate governance. Fox example the Model will be updated in case of an introduction of new activities with impacts on the Predicate offences or in case of reorganization of duties assigned to Departments or Committees.

Therefore, the Board of Directors of Headquarter is responsible for any assessment of the actual implementation of updates, additions and modifications to the Model, also on the basis of the suggestions formulated periodically by the Surveillance Body. In this regard, the Surveillance Body will evaluate the need of any update or amendment to the Model at least once per year.

In any case, the updating activity is aimed at continuously guarantee the adequacy and suitability of the Model, assessed with respect to the preventive commission function of the offences indicated by the Decree.

The Model consists of the set of principles, rules and provisions relating to the management and

control of corporate and instrumental activities and to the implementation and diligent management of a control system for sensitive activities aimed at preventing the commission or attempted commission of the offences provided for in Legislative Decree No. 231/2001.

The following constitute an integral part of the Model:

- Code of Ethics;
- Annex 1 –Risk Assessment & Gap Analysis;
- Internal procedures that also extend their validity to the prevention of offences under the Decree.

In the Branch's operations, the following transversal preventive measures are ensured:

- Power and delegation system: clear and formalised allocation of powers and responsibilities, with express indication of the limits of exercise.
- Segregation of duties: separation of duties and functions through proper distribution of responsibilities and provision of adequate authorisation levels, in order to avoid concentration of sensitive activities on a single person.
- System of controls and monitoring: provision of periodic monitoring/control activities on the operations of the Branch.
- Preservation and traceability of records and documents: preservation and traceability of all activities by means of adequate documentary supports enabling the identification of the persons involved in the operation.
- Periodical monitoring by the Surveillance Body: supervisory activity on the functioning and observance of the measures indicated in the Model.
- Disciplinary system: system suitable for sanctioning non-compliance with the measures indicated in the Model.
- Training and awareness-raising: definition of the methods for ensuring continuous training and awareness-raising of personnel in the areas of operations of the Branch.

In compliance with the provisions of Article 6, paragraph 1, letter a) of the Decree, any subsequent modification, integration and/or updating of the Model - even partial and / or to the individual documents referred to above – will be subject to the Board of Directors of Headquarter’s approval.

CHAPTER 3 - THE SURVEILLANCE BODY

3.1 Identification of the Surveillance Body

In accordance with the Decree, the task of monitoring continuously the Model’s performance, observance and its updating are entrusted to the Surveillance Body, a specific body of the Branch with autonomous powers of initiative and control.

The Surveillance Body must meet the characteristics of autonomy, independence, professionalism and continuity of action. For this purpose, it is provided with powers of initiative and control on

activities of the Branch and has no management or administrative powers.
For ensuring respect of the principle of impartiality/neutrality, the Surveillance Body is placed at the top of the organizational structure of the Branch reporting directly and exclusively to the Board of Directors of Headquarter and informing the General Management of the Branch on a periodical basis.
The Surveillance Body exclusively supervises the observance and the effectiveness of the Model by the Recipients and formulates proposals for the amendment of these objectives, in order to improve its efficiency for what concerns the prevention of crimes included in the list of Predicate offences pursuant to the Decree.
In this context, the Branch has appointed a specific Surveillance Body whose operating mechanisms are governed by the Regulation created for the purpose of determining the frequency of its meetings and audits, the convocation and meeting procedures, the identification of the criteria and procedures for analysis and appointment of the Chairman, etc.

3.2. The Surveillance Body

3.2.1. Composition, appointment, duration and remuneration of the Surveillance Body

In consideration of the governance structure adopted by the Branch, the Surveillance Body is composed of three members, one of whom is external, in order to ensure the autonomy, independence, professionalism and integrity in the exercise of its duties.
The appointment of the Chairman of the Surveillance Body of the Branch is delegated to the Board of Directors of Headquarter.
In particular, the Board of Directors of Headquarter verifies the compliance of the requirements for each new single member of the Surveillance Body to be appointed, by receiving a self-declaration to be issued by such new member of the Surveillance Body to be appointed, confirming his/her compliance with all requirements regarding the eligibility, autonomy and independence, professionalism and continuity of action which are necessary regarding the composition and activity of the Surveillance Body, as well as the absence of any cause for ineligibility and incompatibility. An updated version of the self-certification must be provided to the Board of Directors of the Headquarter each time the appointment as a member of the Surveillance Body is renewed.
In the potential event of revocation, forfeiture or other causes of termination of one or more members, the Board of Directors of Headquarter shall replace the relevant members in compliance with the specialisation criteria and the eligibility requirements set forth under paragraph.
The Surveillance Body shall remain in office for one year.

3.2.2 Requirements

The following are the requirements of eligibility, autonomy and independence, professionalism and continuity of action which are necessary regarding the composition and activity of the Surveillance Body.

3.2.2.1 Subjective requirements of eligibility

The existence of any of the following circumstances constitutes cause for ineligibility for the individual members of the Surveillance Body:

- any cases provided for under Article 2382 of the Civil Code[3];
- situations in which autonomy and independence may be seriously compromised[4];
- indictment for any of the Predicate offences pursuant to the Decree;
- indictment for any crime that is not unpremeditated or that in any case includes disqualification (including temporary disqualification) from public office or executive offices in legal persons.

The members of the Surveillance Body are forced to immediately notify the Chairman of the Surveillance Body and the Board of Directors of Headquarter upon the occurrence of any of the aforesaid circumstances, the occurrence of which represents in itself a cause for immediate and automatic disqualification from office of the member concerned.

As mentioned in paragraph 3.2.1 above, each member of Surveillance Body of the Branch, at least once a year, has to sign an ad hoc declaration in order to guarantee that the subjective requirements of eligibility are respected. In case of occurrence of such circumstance, the Board of Directors of Headquarters shall promptly acknowledge the disqualification and replace the individual in the Surveillance Body.

3.2.2.2 Autonomy and independence

The Surveillance Body of the Branch is provided, within the exercise of its functions, with autonomy and independence from the corporate bodies and other internal control bodies and has also financial independence, based on an annual budget approved by the Board of Directors of Headquarter on the basis of the request made in this regard by the Surveillance Body.

The Surveillance Body has the right, independently and without seeking any prior consent, to dispose of the financial resources indicated in the budget, drawn up on the basis of the planned activities of the Surveillance Body, in relation to which it will submit to the Board of Directors of Headquarter a statement of expenses incurred as part of its annual report.

In the presence of exceptional and urgent situations, the Surveillance Body may use resources in excess of its budget, with the obligation to immediately inform the Chairman of the Board of Directors of Headquarter.

During its audit activities and inspections, the Surveillance Body is granted the widest possible powers in order to carry out its tasks effectively.

In the exercise of their duties, the members of the Surveillance Body must not be in situations, even

[3] Article 2382 of the Civil Code “Causes of ineligibility and revocation” identifies cases in which a person can not be appointed as a director of a company or declines from his office”.

[4] For example, where there is interference from corporate bodies and/or economic or personal conditions that may compromise the autonomy and independence of the Member.

potential situations, where there is a conflict of interest arising from any personal, family or professional reasons. If such situations should occur, the members concerned are forced to immediately inform the other members of the Surveillance Body and to refrain from participating in the relevant decisions.

3.2.2.3 Professionalism

The Surveillance Body must be equipped with at least the following professional skills:

- knowledge of the organization and key business processes;
- legal knowledge that would enable the identification of any cases likely to be considered offences.

In particular, as clarified by practice, the Board of Directors of Headquarter must choose the members of the Surveillance Body by verifying their possession of specific professional skills in relation to risk management and analysis of control systems, inspections, consulting, or knowledge of specific techniques, such as to ensure the effectiveness of the control and proactive powers conferred to it.

If necessary, the Surveillance Body can make use of external consultants also for what concerns the performance of the technical operations necessary to carry out its control function. In this case, consultants must always report the results of their work to the Surveillance Body.

3.2.2.4 Continuity of action

The Surveillance Body must ensure the necessary continuity in the exercise of its duties, also by scheduling its activities and controls, by drafting minutes of its meetings and the regulation of information flows deriving from the corporate structures.

The compliance with these requirements allows the Surveillance Body to:

- continuously check compliance of the Model with the necessary investigative powers;
- verify the effective implementation of the Model, ensuring its continuous updating;
- represent a constant point of contact for all the staff and management of the Branch, promoting the dissemination in the Branch context of knowledge and understanding of the Model.

3.2.3 Grounds for disqualification from office

After their appointment, the Surveillance Body's members shall lapse from office, where:

- one of the requirements needed for eligibility pursuant to the above-mentioned paragraph 3.2.2 named "Requirements" no longer applies;
- there has been an unjustified absence at two or more consecutive meetings of the Surveillance Body, carried out pursuant to a formal and regular convocation.

The members of the Surveillance Body shall immediately notify the Chairman of the Surveillance Body and the Board of Directors of Headquarter of the occurrence of one of the above-mentioned grounds for disqualification from the office.

The Chairman of the Board of Directors of Headquarter shall immediately inform the other members of the Board of Directors of Headquarter at the earliest possible meeting of any occurrence of one of the grounds for disqualification from the office he becomes aware of and shall remove the person concerned from the Surveillance Body and replace him/her.

3.2.4 Grounds for suspension and termination

The conditions set out below are reasons for suspension of a member of the Surveillance Body:

a) a conviction, even if not final, of the member of the Surveillance Body or other sentences would result in suspension from the Board of Directors of Headquarter pursuant to applicable laws;
b) cases in which after being appointed, members of the Surveillance Body are found to have carried out the same role within a Company which has received, by non-final measure, the sanctions laid down in Article 9 of the Decree, concerning unlawful acts committed during their term of office;
c) a non-final sentence, equivalent to the sentence issued pursuant to the Article 444 of the Italian Criminal Procedure Code, even if suspended, for one of the crimes set forth under Legislative Decree 231/01, or under Royal Decree 267/1942 and for tax offences;
d) a request for an indictment for one of the crimes under the Legislative Decree no. 231/01;
e) an illness or accident or other justified impediments that continues for over three months, hindering the member of the Surveillance Body from participating therein.

The affected members of the Surveillance Body shall immediately inform the Chairman of the Surveillance Body and the Board of Directors of Headquarter, under their full responsibility, of the occurrence of one of the above-mentioned grounds for suspension.

Whenever the Chairman of the Board of Directors of Headquarter becomes directly aware of the occurrence of one of the above-mentioned grounds for suspension, shall immediately inform the other members of the Board of Directors of Headquarter which shall, in its next meeting, declare the suspension from office.

In the event of suspension of one or more standing members, the Board of Directors of Headquarter shall promptly identify and order the inclusion in the Surveillance Body of one or more alternate members, taking into account the specific skills of each.

Save for different provisions of laws and regulations, the suspension shall not last more than six months. After this limit has expired and the conditions for suspension are still outstanding, the Chairman of the Board of Directors of Headquarter shall enter the revocation of the suspended member among the items to be addressed in the next meeting.

Members not revoked shall be fully reinstated in office and the replacing alternate member shall cease its position.

The Board of Directors of Headquarter may also terminate one or more members of the Surveillance Body at any time, with just cause:

- if it determines that they have been responsible for gross misconduct in performing their duties, upon prior approval of the Board of Directors of Headquarter, or
- pursuant to a justified resolution or upon a proposal of the Board of Directors of Headquarter, adopted unanimously by all members, for any objective reason referring to the improved application of the Model.

3.2.5 Duties of the Surveillance Body

The Surveillance Body, within its ordinary activities, shall conduct and/or oversee the following tasks:

a) disseminate knowledge and understanding of the Model within the Branch;
b) supervising compliance with the Model and its effective application;
c) monitor the validity and adequacy of the Model, with particular reference to the behaviors identified in the Branch;
d) verify the effective capacity of the Model to prevent the commission of the crimes provided for by the Legislative Decree no. 231/01;
e) propose the update of the Model to the Board of Directors of Headquarter in the event that it is necessary and/or appropriate to make corrections and adjustments of the same, in relation to organisational and/or legislative changes;
f) communicate periodically to the Board of Directors of Headquarter regarding the activities carried out, the reports received, the corrective and improvement actions of the Model and their state of implementation.

To carry out the activities referred to in the previous paragraph, the Surveillance Body shall take the following commitments:

a) spread and verifying within the Branch the knowledge and understanding of the principles contained in the Model;
b) collect, process, store and update any relevant information for the purpose of verifying compliance with the Model;
c) verify and periodically check the areas/ operations at risk identified in the Model;
d) verify and check the regular keeping and effectiveness of all the documentation concerning the activities/operations identified in the Model;
e) set up specific "dedicated" information channels, aimed at facilitating the flow of reports and information to the Surveillance Body;
f) promptly report to the Board of Directors of Headquarter any violation of the Model that is deemed to be found by the Surveillance Body itself, of which it has become aware of the report by the employees or ascertained by the Branch;
g) periodically assess the adequacy of the Model with respect to the provisions and regulatory principles of the Decree and related updating;
h) periodically assess the adequacy of the information flow and adopt any corrective measures;
i) promptly transmit to the Board of Directors of Headquarter all relevant information for the

proper performance of the functions of the Surveillance Body, as well as for the proper fulfillment of the provisions of the Decree;

j) transmit, at least annually, to the Board of Directors of Headquarter a report on the activities carried out, the reports received and disciplinary sanctions (if any) imposed under paragraph 5 below, the necessary and/or appropriate corrective and improvement actions of the Model and their status of realization.

3.2.6 Control of the adequacy and compliance of the Model

In order to verify the adequacy and functioning of the Model, the Surveillance Body provides for the preparation of an Annual Plan aimed at identifying the Risky Areas and Risky Activities identified in the Model and the efficiency of the protocols adopted by the Branch to oversee the same, also through periodic checks not previously communicated.

The Surveillance Body is also entitled to provide for the request, collection and processing of any relevant information for the purpose of verifying the adequacy and compliance of the Model by recipients.

The verification takes place through the establishment of specific "dedicated" information channels aimed at facilitating the flow of reports and determining the methods and frequency of the transmission.

With regard to the verification and updating of the Model, the Surveillance Body in particular:

- monitors the evolution of the reference legislation and consequently prepares suitable measures to keep the mapping of the activities at risk up to date, according to the methods and principles followed in the adoption of this Model;
- monitor the adequacy and updating of protocols aimed at preventing crimes and verifies that each part of the Model is adequate for the purposes identified by law;
- in the case of commission of offences and violations of the Model, evaluates the opportunity to introduce changes to the Model, submitting them to the approval of the Board of Directors of Headquarter;
- verifies that the modifications to the Model are effective and functional;
- oversees the delegation system adopted by the Branch to ensure the effectiveness of the Model, also through cross-checking checks;
- promptly transmits to the Board of Directors of Headquarter all relevant information for the correct execution of its functions and for the correct fulfilment of the provisions contained in the Decree.

With regard to compliance responsibilities, the Surveillance Body checks the regular maintenance of all documentation concerning the activities and operations identified in the Model.

The Surveillance Body may dispose of the investigations aimed at assessment possible violations of the provisions of the Model, also on the basis of the reports received. The identified infringements

are reported to the competent body for the opening of the disciplinary procedure, also verifying that the violations of the Model are effectively and adequately sanctioned.

3.2.7 Powers of the Surveillance Body

The Surveillance Body has free access to any document relevant for the performance of the functions assigned to it by the Decree.

Moreover, to allow the Surveillance Body to fulfill its obligations, the Surveillance Body are empowered with the following powers:

- to issue provisions and service instructions aimed at regulating the activity of the Surveillance Body;
- to request the cooperation of internal structures or highly professional external consultants and demonstrated competence in cases where this is necessary for the performance of their duties;
- to be promptly provided with all the data and/or information required to identify aspects elated to the various activities relevant to the Model and to verify the effective implementation of the same by the Branch's organizational structures;
- to supervise the correctness of the sanctions system, including the proposal of sanctions to be evaluated and applied by the Branch in case of severe and/or material breach of the 231 protocols;
- to carry out audits and inspections, even without prior notice;
- to dispose of the financial resources made available to the Surveillance Body for the performance of its activities;
- to proceed, if necessary, to directly hear/request information from the employees of the Branch.

The Surveillance Body to perform its tasks more effectively may decide to delegate one or more specific obligations to individual members. In any case, the liability arising out of these functions falls to the Surveillance Body as a whole.

3.2.8 Information flows to the Surveillance Body

The Surveillance Body must transmit promptly all relevant information to the Board of Directors of Headquarter for the proper performance of its functions, as well as for the proper fulfillment of the provisions of the Decree. For this purpose, the Surveillance Body has set up a specific "dedicated" information channel, aimed at facilitating the flow of reports and information to the Surveillance Body. In particular, the concerned Departments of the Branch are requested to transmit to the Surveillance Body "event-based" information flows and "periodic" information flows in accordance with the document by the Surveillance Body.

The Surveillance Body has the power to arrange that the recipients of its requests promptly provide the information, data and/or information required to identify aspects related to the various activities

relevant to the Model.

The members of the Surveillance Body are bound to secrecy regarding the news and information acquired in the exercise of their functions. This obligation, however, does not exist with respect to the Board of Directors of Headquarter.

3.2.8.1 Information duties relating to official acts

The Surveillance Body must create a system that allows Senior person, Non-Manager Employees and External Parties to report illicit conduct realized in the performance of their work, ensuring the confidentiality of the name of the person making the report. The Surveillance Body is entrusted with the task of verifying any unlawful conduct held by all the subjects that collaborate with the Branch.

For the proper exercise of its powers, to the Surveillance Body is mandatory and promptly provided with any information concerning:

1) the provisions and/or news concerning the existence of a criminal proceeding (even if registered in relation to unknown persons or persons to be identified or as an "act not constituting criminal offences"), relating to facts of interest for the Branch;
2) the provisions and/or news concerning the existence of administrative proceedings or significant civil disputes, relating to requests or initiatives by independent Authorities, the financial administration, local administrations, contracts with the Public Administration, requests and/or management of public funding;
3) requests for legal assistance forwarded to the Branch by the staff in case of criminal or civil proceedings against them;
4) the reports prepared by the Heads of the Departments of the Branch in the context of their control activities which may reveal facts that present significant profiles for the purposes of compliance with the Model.

Finally, the Surveillance Body must be promptly notified of the system of delegation adopted by the Branch and any changes that affect it.

3.2.8.2 Reports from employees of the Branch or Third parties

In addition to the mandatory information flows referred to above, the Surveillance Body identifies any further information, relevant for verifying the adequacy and compliance with the Model, which must be transmitted to it by the recipients of the same.

As regards the reporting process by employees and Third parties:

- in compliance with the provisions of the Model, in consideration of the Whistleblowing Policy, the Surveillance Body may receive whistleblowing reports from the Whistleblowing Officer pertaining to the violations of the Model;
- subject to the provisions of the law to protect the reputation of the Branch and any interested parties, the Surveillance Body, in coherence with the provisions of the Model and the Whistleblowing Policy, guarantees the confidentiality of the identity of the whistleblower, and

those who dutifully cooperate in their investigation, and sees that, by reason thereof, the same are not retaliated, discriminated, penalized and other negative consequences;

- all the reports and information acquired must be conserved for a period of five (5) years in a dedicated archive maintained by the Surveillance Body, regulating its access by other corporate bodies who makes a justified request.

In any case, each Department Head must inform the Surveillance Body of any anomaly or breach of the Model found in the course of the checks carried out on the area/activity for which he/she is responsible.

3.2.9 Reporting by the Surveillance Body towards the Board of Directors of Headquarter

In order to guarantee its entire autonomy and independence in carrying out its duties, the Surveillance Body reports periodically to the Board of Directors of Headquarter.

The Surveillance Body constantly reports to the Board of Directors of Headquarter on:

- the activities carried out, the reports received and the disciplinary sanctions (if any) imposed pursuant to paragraph 5 below, together with the necessary and/or opportune corrective and improvement actions of the Model and their state of realization;
- the updates to be made to the "Organizational, Management and Control Model" in order to guarantee the monitoring of risks deriving from the offences envisaged by the Decree.

The Surveillance Body also draws up a general report on its work and its management of expenses which – at least annually - is brought to the attention of the Board of Directors of Headquarter, contents of this report and audit activities planned for the following year are explained in a dedicated meeting.

3.2.10 The internal system for reporting violations (Whistleblowing)

The Branch attributes to the system of internal reporting a great value in order to promote behavior in line with their ethical principles. All the employees are encouraged to report any of these behaviours not in line with the ethics of the Branch through the reporting channels set out in the Whistleblowing Policy.

However, in the case of an employee may feel unable or uncomfortable raising a concern through the normal reporting channels, the Branch provides a means for all employees (being permanent, temporary or under any contractual agreement) working for and/or on behalf of the Branch to report, anonymously.

The Branch is committed to preventing any retaliatory action (e.g. dismissal, downgrading, change of working hours) against whistleblowers.

The Branch has adopted a Whistleblowing Policy in order to ensure that the management of whistleblowing is carried out in compliance with the regulations in force.

The Branch has appointed the Head of Legal & Compliance Department as “Whistleblowing Officer”, with the tasks of:

- Receiving concerns from and communicating with (potential) Whistleblowers;

- Conducting a preliminary investigation;
- Providing information to the authorized persons based on a strict “need to know”.

In the event that the reports relate to the Head of Legal & Compliance Department, the whistleblower must report the matter to the European Chief Compliance Officer in Luxembourg.

If a breach is established, the General Management of the Branch may decide on possible disciplinary sanctions, in coordination with the Head of the General Administration Department of the Branch.

Any documentation supporting the concern and/or any communication internally exchanged shall be retained and deleted in accordance with the applicable law and/or regulations governing the document retention and destruction requirements.
This procedure covers reports of irregularities or misconduct of a general, operational or financial nature within the Branch, including, but not limited to, notices about irregularities or suspicions of irregularities or misconduct of a general, operational or financial nature within the Branch relating to the:

- criminal activity (such as embezzlement, theft, money laundering, fraud etc.);
- breaches of the Branch’s policies and procedures (including the 231 Model), customer treatment standards, etc.;
- manipulating procedures / Manipulating IT systems to achieve product sales, targets or bonuses;
- breaches of national and European regulatory or legal requirements, with particular focus on banking and financial framework;
- breaches of the Branch’s financial accounting and auditing obligations;
- breaches of Market Abuse Regulation, including: insider dealing, unlawful disclosure of inside information and market manipulation;
- bribery and corruptions practices;
- altering or removing remitter of beneficiary information in payment instructions to avoid the detection of sanctioned individuals, entities or jurisdictions;
- other risks or dangers at work including IT security;
- any behavior endangering the staff health and safety, as well as the environment;
- any attempt to conceal information relating to an illegal activity detected regarding any of the above points.

Employees of the Branch are encouraged to report any notices by:

- postal mail
- telephone line in person.

CHAPTER 4 - INTERNAL TRAINING AND COMMUNICATION

4.1 Introduction

The administrative liability regime laid down by the Italian law and the “Organisational, Management and Control Model” adopted by the Branch forms an overall system, which must be reflected in the operational conduct of the Branch’s Staff.

The Branch, aware of the importance of the training and information aspects, operates in order to ensure that its staff is aware of both the content and obligations under the Decree and the Model.

In order to obtain a Staff aware of ethics and the conduct to be held within the Branch is essential to implement a communication and training activity for the purpose of disseminating the contents of the Decree and of the Model adopted, including all its various components (the corporate instruments underlying the Model, the aims of the Model, its structure and key components, the powers and delegation system, identification of the Surveillance Body, information flows to the Surveillance Body, the protections provided to those that report unlawful acts, etcetera). The purpose is to ensure that knowledge of the subject matter and compliance with the rules arising from it become an integral part of each Staff member’s professional culture.

Based on this knowledge, the training and internal communications activities addressed to all the Staff have the constant objective – also in accordance with the specific roles assigned – of creating a widespread knowledge and a corporate culture embracing the issues in questions, having regard to the specific activities carried out, so as to mitigate the risk of offences taking place.

4.2. Internal communication and communication to external parties

The principles and rules contained in the Model and any modification, integration and / or update are made available to the attention of all External Parties who collaborate with the Branch with appropriate training and/or communication initiatives, differentiated according to the role and the responsibility of the recipients.

These initiatives are included in the training program concerning the "Discipline of the administrative responsibility of legal entities, companies and associations also without legal personality". The programme includes a training course that employees must actually attend and a final test that must be taken and passed.

In accordance with the above purposes, the Surveillance Body carries out:

- **Information activities**: the adoption of this document and any modification, integration and/or update are communicated to all the resources of the Branch at the time of adoption and/or modification. The new resources are given an information set, containing the text of the Decree, the present document "Organisational, Management and Control Model” pursuant to Legislative Decree 231/2001", the Code of Ethics and the Staff Handbook, so as to ensure the knowledge referred to above;
- **Training activities**: this activity is carried out with a periodic training to the employees and

also with updating meetings and seminars;

- **Verification activities**: the Surveillance Body may provide for specific controls - also by sample tests or assessment and self-assessment tests - aimed at verifying the quality of the content of the training programs and the effectiveness of the training provided.

As regards the communication to External Parties, the Branch promotes the knowledge and observance of the Model also among commercial and financial partners, consultants, collaborators in various capacities, customers and outsourcers. For example, the adequate communication methods adopted by the Branch, in accordance with the best practice, are the publication of the Model 231 on the website of the Branch and inclusion in contracts concluded by the Branch a specific clause concerning compliance with the regulatory provisions provided for by the Legislative Decree n. 231/2001.

CHAPTER 5 - THE DISCIPLINARY SYSTEM

5.1 General Principles

In addition to the adoption of decision-making and control mechanisms such as to eliminate or significantly reduce the risk of commission of the criminal offences and administrative infringements covered by the Decree, the Model effectiveness is ensured by the disciplinary instruments established in order to control and penalize improper behaviors.

Articles 6 (para. 2, letter e) and 7 (para. 4, letter b) of the Decree provide that organisational and management models must introduce a disciplinary system capable of sanctioning non-compliance with the measures indicated therein.

Any conduct of the employees of the Branch and of External parties which are not in line with the principles and the rules of conduct laid down in this Model – including, but not limited to, the Code of Ethics, the Code of Conduct of ICBC (Europe) S.A. and the internal procedures and rules, which are an integral part of the Model – shall constitute a breach of contract.

In compliance with Art. 21 of Legislative Decree 24/2023 "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and on the protection of persons who report breaches of national laws", the Branch has provided in its disciplinary system for sanctions for those who are responsible for the breaches provided thereby that damage its integrity.

Based on this premise, the Branch shall adopt:

- towards its Employees in service through a contract governed by the Italian law and through the CCNL, the system of sanctions laid down in the applicable laws and regulations (including the CCNL itself and the relevant Workers' Statute "*Statuto dei Lavoratori*");
- towards External Parties, the system of sanctions laid down in the contractual and legal

provisions governing this area.

The General Administration Department, after consultation with the General Management, within the limits of its competences and on the basis of the reports submitted by the Surveillance Body, initiates, implements and concludes disciplinary proceedings against employees.

The penalties against External Parties shall be implemented, according to the contractual provisions regulating the services, by the General Administration Department, after consultation with the General Management.

The type and size of each of the sanctions established shall be defined, pursuant to the above-mentioned legislation, taking into account:

- the degree of imprudence, lack of judgment, negligence, fault, or bad faith of the conduct relating to the action/omission, also considering any reiteration of the misconduct;
- the activity carried out by the person concerned and his functional position;
- any other relevant circumstances.

Such disciplinary action shall be pursued regardless of the initiation and/or performance and finalization of any criminal judicial action, since the principles and the rules of conduct laid down in the Model are adopted by the Branch in full autonomy and independently of any criminal offences which said conduct may determine and which it is for the judicial authority to ascertain.
Therefore, in application of the above-mentioned criteria, the following system of sanctions is established.
The Surveillance Body is responsible for verifying the adequacy of the system of sanctions and constantly monitoring the application of sanctions to employees and the actions in respect of External Parties. To this end, the General Administration Department, which, at least once a year, indicates the disciplinary measures taken against employees during the reference period within the “information flow” template sent to the Surveillance Body on a quarterly basis.
The system of sanctions envisaged for employees serving under an employment contract governed by Italian law is detailed below.

5.2 Employees without managerial positions

The conduct of Non-Manager Employees that is in breach of the rules of conduct contained in the Model and the Code of Ethics constitutes non-compliance with a primary employment obligation and, consequently, constitutes disciplinary offences.
The penalty applied must be proportional to the seriousness of the breach committed, and, in particular, must take into consideration:

- the intentionality of conduct or the degree of guilt (negligence, carelessness or incompetence);
- any previous misconduct and disciplinary sanctions imposed on the employee;
- the level of responsibility and autonomy of the employee who committed the disciplinary

offense;

- the involvement of other persons;
- the level of risk to which the Company may reasonably be exposed following a breach;
- other particular circumstances

The General Administration Department of the Branch, after examining the elements mentioned above and after consultation with the General Management, has at its disposal the following sanctioning measures:

- **Verbal warning**: shall apply in the event of minor breach of the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the Risky Activities, of a conduct which is not in line with or not appropriate to the requirements of the Model.
- **Written warning:** shall apply in the event of failure to comply with the principles and of rules of conduct laid down in this Model or breach of the internal rules and procedures set out and/or referred to, or adoption, within the Risky Activities, of a conduct which is not in line with or not appropriate to the requirements of the Model, where such non-compliance is assessed to be neither minor nor serious.
- **Suspension from work without pay for up to 10 days**: shall apply in the event the minor breaches mentioned in sub-paragraph relating to the Verbal Warning above are repeated by the relevant employee at least twice in the preceding two years.
- **Dismissal for substantiated reasons:** shall apply in the event of adoption, in performance of the activities belonging to the Risky Areas, of a conduct characterized by serious non-compliance with the requirements and/or the procedures and/or the internal rules laid down in this Model where it is even simply liable to give rise to one of the offences covered by the Decree.
- **Dismissal with cause:** shall apply in the event of adoption, in performance of the Risky Activities, of a conduct willfully in contrast with the requirements and/or the procedures and/or the internal rules laid down in this Model, which, although it is simply liable to give rise to one of the offences covered by the Decree, impairs the relationship of mutual trust which characterises employment relationships, or is so serious as to impede continuation of employment, even temporarily.

5.3 Managers

Where Senior positions / senior persons infringe the internal principles, rules and procedures set out in this Model or adopt, in performing the activities belonging to the Risky Areas a conduct not in line with the requirements of the Model, such persons shall incur the measures indicated below, which shall be applied having due regard to the seriousness of the infringement and to whether it is a repeat occurrence. Also, in consideration of the particular fiduciary relationship existing between the Branch and executive level employees, in compliance with the applicable provisions of the law and with the

CCNL for Executives in credit Companies, dismissal with notice and dismissal with cause shall be applicable for the most serious infringements.

As said measures involve termination of the employment relationship, the Branch, acting in accordance with the legal principle of applying a graduated scale of sanctions, reserves the right, for less serious infringements, to apply the written warning – in cases of mere failure to apply the principles and rules of conduct set out in this Model or of infringement of the internal rules and procedures set out and/or referred to, or of adoption, within the Risky Areas, of a conduct non complying with or not appropriate to the requirements of the Model – or alternatively, to apply suspension from work without pay for up to 10 days – in the event of negligent infringement of duty to a non-negligible degree (and/or repeated) or of negligent conduct infringing the principles and rules of conduct provided for by this Model.

5.4 External parties

Any conduct adopted by External Parties in conflict with this Model, may give rise to the risk of occurrence of one of the offences covered by the Decree, shall, in accordance with the specific terms and conditions of contract included in the letter of appointment or in the agreement, produce early termination of the contractual relationship, without prejudice to any further remedy available to the Branch in the event that it suffers real damage as a consequence of such conduct (i.e. where the Judicial Authority applies the sanctions set out in the Decree).

SPECIAL PART

Introduction to the Special Part of the Model

This Special Partis an integral part of the Organization, Management and Control Model adopted by ICBC (Europe) S.A. Milan Branch, pursuant to and for the purposes of Article 6 of Legislative Decree no. 231/01.

In consideration of the analysis of the structure, the areas of operation, the processes of the Branch, all the types of crime included in the Decree could be abstractly realized and however, the following individual Section of the Special Part examine and analyze the categories of offence considered particularly relevant as a result of Risk Assessment activities.

In addition, with reference to:

- Crimes against female genital mutilation practices (referred to in article 25-quater.1 of the Decree);
- certain Crimes against the individual (Articles 600, 600-bis, 600-ter, 600-quater, 600-quinquies, 609-undecies of the Criminal Code, provided for in Article 25-quinquies of the Decree);
- Counterfeiting and / or sanitary adulteration (Law No. 9/2013 art. 12);
- Fraud against the European Agricultural Fund (L. No. 898/1986. Article 2).

the Branch considered that the significant risks of committing such crimes are only abstractly and not concretely conceivable and, in any case, excluded from the business activity perimeter of the Branch or extraneous to the banking context and in any case to the ordinary operations of the Branch;

In these areas, due to the values set out in the Code of Conduct, the sector to which it belongs and the type of business of the Branch, it appears in fact difficult to configure a liability under the Decree, both because of the difficulty of assuming that the aforesaid offences could come into existence in the banking sector, and because of the difficulty of identifying, even if such offences were committed, any interest or advantage of the Branch.

Moreover, the applicability of the offence referred to in Article 1 of the 2019 Decree-Law (the so-called Cybersecurity Decree), converted with amendments by Law No. 133/2019, referred to in Article 24 bis of the Decree as a predicate offence, was also excluded.

On the basis of these considerations, the Branch has therefore deemed it reasonable not to identify, with respect to the aforementioned offences, any specific organisational safeguards, without prejudice in any case to the obligation for anyone acting in the name and on behalf of the Branch to always operate in compliance with the law and the principles of ethics, integrity, fairness and transparency.

In any case, the preventive measures adopted by the Branch in order to prevent the crimes detailed in the individual Sections of the Special Part, can constitute - in compliance with the Code of Conduct,

Code of Ethics and legislative provisions - an adequate control also for the prevention of these crimes; any criminal conduct that's classifiable as a crime (so including those not classifiable as Predicated Offence) or committed within the premises of the branch, shall be promptly evaluated to be reported through the ordinary means to the judicial authorities (noticed or exposed to the authority).

The categories of offence considered particularly relevant as a result of Risk Assessment activities are the following:

- offences against the Public Administration (Articles 24 and 25, Decree);
- computer crimes and unlawful data processing (Article 24-bis, Decree);
- organised crime offences (Article 24-ter, Decree);
- offences relating to counterfeiting money, public credit cards, revenue stamps and identification instruments or signs (Article 25-bis, Decree);
- offences against industry and trade (Article 25-bis.1, Decree);
- corporate offences (Article 25-ter, Decree);
- offences with the purpose of terrorism or subversion of the democratic order (Article 25-quater, Decree);
- offences against the individual (Article 25-quinquies, Decree);
- market abuse offences (Article 25-sexies, Decree);
- offences of manslaughter or serious or very serious injury, committed in violation of the rules on the protection of health and safety at work (Article 25-septies, Decree);
- offences of receiving, money laundering and use of money, goods or benefits of unlawful origin, as well as selflaundering (Article 25-octies, Decree);
- offences relating to non-cash payment instruments (Article 25-octies.1);
- offences relating to violation of copyright (Article 25-novies, Decree);
- offences of inducement not to make statements or to make false statements to the judicial authorities (Article 25-decies, Decree);
- offences against the environment (Article 25-undecies, Decree);
- offences of employing citizens of third countries whose stay is irregular (Article 25-duodecies, Decree).
- racism and xenophobia (Article 25-terdecies, Decree);
- fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited devices (Article 25-quaterdecies, Decree);
- tax offences (Article 25-quinquesdecies, Decree)
- offences against cultural heritage (Article 25-septiesdecies, Decree);
- laundering of cultural assets and devastation and looting of cultural and landscape assets (Article 25- duodevicies, Decree).

Transnational offences (Law No. 146/2006) are by definition offences that occur when there is a stable criminal organisation even outside national borders, and therefore extend the pervasiveness of the risk to all mapped areas.

These offences are to be understood as all risk areas, sensitive activities, and the relevant control measures.

Each individual Section of the Special Part of the Model is composed of the following paragraphs:

- Introduction: dedicated to the description and reference legislation governing the crimes included in that Section of the Special Part;
- General rules of conduct: referring the principles set out in the Code of Ethics, the Code of Conduct and specific policies / procedures, this paragraph lays down the general rules of conduct which must inspire the behavior of the recipients of the Model in order to prevent the commission of the crimes;
- Risky activities and instrumental processes pursuant to Legislative Decree no. 231/01 and main methods of committing offences: includes all risky activities which, following the risk analysis carried out on the Branch, have been identified as risky for that specific family of crime. In addition, for each risky activity is indicated an example of conduct which could integrate the crime and the preventive measures that the Branch has adopted in order to mitigate the possible commission.

The Head of General Administration Department shall pay the strictest attention to the dissemination of this document and the Code of Ethics to all the members of the Department coordinated. The same attention shall be paid whenever the composition of the staff changes as a result of internal movements or new hirings.

Any failure to comply with this document shall result in disciplinary sanctions in accordance with the law, the contractual provisions in force and the Code of Conduct adopted by the Branch.

FIRST SECTION - OFFENCES AGAINST THE PUBLIC ADMINISTRATION

1.1. Introduction

Articles 24 and 25 of the Decree concern a series of offences laid down in the Criminal Code which have in common the protection of the impartiality and sound management of the Public Administration.

Specifically, the offences against the Public Administration, set out in Articles 24 and 25 of the Decree, include:

Art. 24 - Misappropriation of public funding, fraud against the State or a public body or the European Union or to obtain public funding or IT fraud against the State or against a public body or fraud in public supply:

- **Embezzlement to the detriment of the State (Article 316-bis of the Criminal Code):**

anyone who, having obtained from the State or from another public body or from the European Communities grants, subsidies, financing, subsidised loans or other disbursements of the same type, however named, intended for the achievement of one or more purposes, does not use them for the intended purposes, shall be liable for this offence.

- **Unlawful receipt of public grants to the detriment of the State (Article 316-ter of the Criminal Code):** this offence is committed by any person who, through the use or presentation of false declarations or documents or certifying untrue things, or through the omission of required information, unduly obtains, for himself or others, contributions, subsidies, loans, subsidised mortgages or other funds of the same type, however denominated, granted or disbursed by the State, other public bodies or the European Communities.
- **Fraud to the detriment of the State or other public body or of the European Communities (Article 640 of the Criminal Code):** anyone who, through artifice or deception, misleading the State or a public body, procures an unjust profit for himself by causing damage to the State or the public body, shall be liable for this offence.
- **Aggravated fraud for the obtainment of public funds (Art. 640-bis of the Criminal Code):** a precondition of the offence is that the fraud concerns the disbursement of subsidies, financing, subsidised loans or other disbursements of the same type, granted or disbursed by the State, public bodies or the European Communities.
- **Computer fraud if committed to the detriment of the State or of another public body (Article 640-ter of the Criminal Code):** anyone who, by altering in any way the operation of a computer or telecommunications system or by intervening without the right to do so in any manner whatsoever on data, information or programmes contained in a computer or telecommunications system or pertaining thereto, procures for himself or others an unjust profit to the detriment of the State or of another public body shall be liable for this offence.
- **Fraud in public supply (Article 356 of the Criminal Code):** anyone who, in the performance of supply contracts with the State, with another public body or with a company providing public services or services of public necessity, fails to fulfil his obligations by resorting to artifice or deception so as to deceive the other party as to the content of his performance, by causing the lack of all or part of things or works necessary for a public establishment or a public service, shall be liable for this offence.
- **Fraud to the detriment of the European Agricultural Fund (Article 2 of Law No. 898/1986):** this offence is committed by any person who, by presenting false data or information, unduly obtains for himself or others aid, premiums, allowances, refunds or disbursements in general charged in whole or in part to the European Agricultural Guarantee Fund or the European Agricultural Fund for Rural Development. These disbursements are assimilated to the national complementary shares of those disbursed by the aforesaid Funds

as well as to the disbursements charged in full to the national finance on the basis of Community legislation.

- **Disturbing the freedom of public tenders (Article 353 of the Criminal Code):** this offence is committed by any person who, by means of violence or threats or by means of promised collusion or other fraudulent means, prevents or disrupts tenders in public tenders or private tenders on behalf of public administrations, or drives away the bidders.
- **Obstructing the procedure for the choice of contractor (Article 353-bis):** unless the offence constitutes a more serious offence, anyone who, by means of violence or threats or by promises of collusion or other fraudulent means, disrupts the administrative procedure aimed at establishing the content of the call for tenders or other equivalent act in order to influence the manner in which the public administration chooses the contractor shall be liable for this offence.

Article 25 - Embezzlement, Concussion, undue inducement to give or promise benefits, and Bribery and office abuse:

- **Concussion (Article 317 of the Criminal Code):** this offence is committed by a public official who, abusing his position or powers, compels someone to give or promise unduly, to him or to a third party, money or other benefits.
- **Bribery relating to the exercise of duties (Article 318 of the Criminal Code):** the public official who, in the exercise of his functions or powers, unduly receives, for himself or a third party, money or other benefits or accepts the promise thereof is liable for this offence.
- **Bribery relating to an act contrary to official duties (Article 319 of the Criminal Code):** the public official who, in order to omit or delay or to have omitted or delayed an act of his office, or in order to perform or to have performed an act contrary to official duties, receives, for himself or for a third party, money or other benefits, or accepts the promise thereof, shall be liable for this offence.
- **Bribery in judicial proceedings (Article 319-ter of the criminal code):** this offence occurs when the facts indicated in Articles 318 and 319 are committed to favour or damage a party in a civil, criminal or administrative trial.
- **Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code):** this offence is committed by a public official or a person in charge of a public service who, abusing his position or powers, induces someone to give or promise unduly, to him or to a third party, money or other benefits.
- **Corruption of a person in charge of a public service (Article 320 of the Criminal Code):** this provision provides that the provisions of Articles 318 and 319 also apply to a person in charge of a public service.
- **Penalties for the corruptor (Article 321 of the Criminal Code):** this provision provides that the penalties laid down in the first paragraph of Article 318, Article 319, Article 319-bis, Article

319-ter, and Article 320 in relation to the aforementioned cases of Articles 318 and 319 also apply to the person who gives or promises the public official or the person in charge of a public service money or other benefits.

- **Incitement to bribery (Article 322 of the criminal code):** anyone who offers or promises money or other benefits not due to a public official or a person in charge of a public service or for a corrupt purpose but the offer or promise is not accepted shall be liable for this offence.
- **Embezzlement, extortion, undue inducement to give or promise benefits, bribery and incitement to bribery, abuse of office, of members of international courts or bodies of the European Communities or of international parliamentary assemblies or international organisations and of officials of the European Communities and of foreign States (Art. 322-bis of the Criminal Code):** this offence is committed when the offences of embezzlement, extortion, undue induction to give or promise benefits, bribery, abuse of office and incitement to bribery are committed by members of Community institutions (e.g. European Commission, European Parliament, Court of Justice, Court of Auditors).
- **Traffic of illicit influences (Article 346-bis of the Criminal Code):** this offence is committed by any person who, apart from cases of complicity in the offences referred to in Articles 318, 319, 319-ter and in the corruption offences referred to in Article 322-bis, by exploiting or boasting existing or alleged relations with a public official or a person in charge of a public service or one of the other persons referred to in Article 322-bis unduly causes to be given or promised, either to himself/herself or to others, money or other benefits, as the price of his/her unlawful mediation towards a public official or a person in charge of a public service or one of the other persons referred to in Article 322-bis, or to remunerate him/her in connection with the exercise of his/her functions or powers.
- **Embezzlement (limited to the first paragraph) (Article 314 of the Criminal Code):** a public official or a person in charge of a public service, who, having by reason of his office or service the possession or otherwise the availability of money or other movable property of others, appropriates it, is liable for this offence.
- **Embezzlement by profiting from the error of others (Art. 316 of the Criminal Code):** the public official or the person in charge of a public service, who, in the exercise of his functions or service, benefiting from the error of others, unduly receives or retains, for himself or for a third party, money or other benefits, shall be liable for this offence.
- **Office abuse (Article 323 of the Criminal Code):** this offence is committed by any public official or person in charge of a public service who, in the performance of his duties or service, in breach of specific rules of conduct expressly laid down by law or by acts having the force of law and from which no margin of discretion remains, or by failing to abstain in the presence of his own interest or that of a close relative or in the other prescribed cases, intentionally

procures for himself or others an unfair pecuniary advantage or causes unfair damage to others.

The "active subjects" for the purposes of the Decree, i.e., those subjects whose qualification is necessary to integrate the criminal offences set out in the Decree, are the figures of "Public Officials" and "Persons in Charge of a Public Service".

Public Officials

Pursuant to Article 357(1) of the Criminal Code, a public official for the purposes of criminal law is “any person who exercises a legislative, judicial or administrative public function”.

The second paragraph then goes on to define the notion of 'public administrative function'.

No similar definitional activity has been undertaken, however, to specify the notion of legislative and judicial functions since the identification of the persons exercising them respectively has not usually given rise to particular problems or difficulties.

Accordingly, the second paragraph of the article under review specifies that, for the purposes of criminal law, “an administrative function is a public function governed by rules of public law and authoritative acts and characterised by the formation and manifestation of the will of the public administration or by its performance by means of authoritative or certifying powers”.

This last regulatory definition identifies, first of all, the 'external' delimitation of the administrative function. This delimitation is implemented through recourse to a formal criterion that refers to the nature of the discipline, whereby an administrative function is defined as public if it is governed by “public law rules”, i.e. by those rules aimed at the pursuit of a public purpose and the protection of a public interest and, as such, opposed to private law rules.

The second paragraph of Art. 357 of the Criminal Code then translates into regulatory terms some of the main criteria identified by case law and doctrine to differentiate the notion of “public function” from that of “public service'”.

Therefore, “public functions” are peacefully defined as those administrative activities that respectively and alternatively constitute the exercise of:

- Deliberative powers
- Authoritative powers
- Certifying powers

In the light of the principles set out above, it can be said that the most problematic category of subjects is certainly those who perform a “public administrative function”.

In order to provide a practical contribution to the resolution of any "doubtful cases", it may be useful to recall that the qualification of public officials is assumed not only by persons at the top political administrative level of the State or of territorial entities, but also - always referring to an activity of another public entity governed by public law - by all those who, on the basis of the statutes and the delegations that they allow, legitimately form the will and/or carry it out externally by virtue of a power

of representation.
Other persons who, albeit of a far from modest degree, perform only preparatory tasks for the formation of the will of the body (and thus administrative secretaries, surveyors, accountants and engineers, unless, in specific cases and for individual tasks, they do not 'form' or manifest the will of the public administration) do not therefore assume the qualification in question.

Persons in charge of a public service

The definition of the category of “persons in charge of a public service” can be found in Art. 358 of the Criminal Code, which states that “persons in charge of a public service are those who, for whatever reason, perform a public service”.
A public service is to be understood as “an activity governed in the same manner as a public function but characterised by the lack of the powers typical of the latter and excluding the performance of simple tasks of order and the performance of merely material work”.
The legislator specifies the notion of 'public service' by means of two orders of criteria, one positive and one negative. In order for the “service” to be defined as public, it must be governed - like the “public function” - by public law rules, but with the differentiation relating to the absence of the certifying, authorising and deliberative powers proper to the public function.

The legislature also specified that the performance of “mere orderly tasks” or the “performance of merely material work” can never constitute a “public service”. With reference to the activities that are carried out by private entities on the basis of a concessionary relationship with a public entity, it is considered that for the purposes of defining as a public service the entire activity carried out in the context of that concessionary relationship, it is not sufficient the existence of an authoritative act of subjective investiture of the public service, but it is necessary to ascertain whether the individual activities that are in question are themselves subject to a public-type discipline
Case law has identified the category of persons entrusted with a public service, emphasising the character of the instrumentality and ancillary nature of the activities in relation to the public service in the strict sense
It has therefore indicated a series of “revealing indices” of the public nature of the entity, for which the case law on the subject of joint-stock companies with public shareholdings is emblematic. In particular, reference is made to the following indices:

- Subjection to a control and guidance activity for social purposes, as well as to a power of appointment and revocation of directors by the State or other public bodies
- The presence of a convention and/or concession with the public administration
- The financial contribution by the State
- The immanence of the public interest within the economic activity

On the basis of the above, it could be argued that the discriminating element in indicating whether or not a subject has the status of 'entrusted with a public service' is represented, not by the legal

nature assumed or held by the entity, but by the functions entrusted to the subject, which must consist in the care of public interests or the satisfaction of needs in the general interest

One should therefore always carefully examine the type of relationship one has with a third-party entity and in case of doubt as to its legal nature, immediately contact the Head of the Legal & Compliance Department for further investigation and clarification.

1.2. General rules of conduct

In order to operate in compliance with the provisions of law and ethics, payments or fees, in any form, offered/promised for the purpose of facilitating or remunerating a decision or the comply with an official act or an act contrary to the official duties of the Public Administration are strictly prohibited. The prohibition concerns payments or fees made directly or through an individual or legal person.

It is also strictly forbidden to engage in the same conduct for the purpose of favoring or damaging a party in a civil, criminal or administrative case, and bring a direct or indirect advantage to the Branch.

The practices of corruption, illegitimate favors, collusive behavior, direct or indirect solicitations, of undue advantages, as well as any behavior capable of causing unjust damage to the State, to the European Union or to other public bodies, are absolutely prohibited.

All conducts aimed at receiving and/or gaining an illicit public contribution, even referring to and including those related to the European Community (EU), and to carry out illegal conducts, even if required by any public official, are strictly prohibited, if they are in breach of current laws and regulation and might constitute a potential source of illegal economic advantage.

The Branch, in its relations with representatives, officials or employees of the Public Administration, is committed:

1. to prohibit the attempt and/or establishment of personal relations of favor, influence or interference that could directly or indirectly influence the relationship;
2. to prohibit the offering of money, goods or other benefits to representatives, officials or employees of Public Administrations, including also those conferred through a third party.
3. to prohibit the offer or acceptance of any object, service, performance or form of courtesy in order to obtain more favorable treatment in relation to any relationship with the Public Administration; in the same way, it is forbidden to offer other benefits which may also take the form of job or commercial offers to the Public Official, to his family members or to persons in any way connected with him.

Minor non-monetary gifts may be an exception, and therefore be accepted according to the approval process set out in the Gifts and Entertainment Policy, if they are of modest value and the circumstances do not suggest that they are intended to obtain undue favors. In particular, if they are non-cash gifts of nominal value; customary and reasonable meals and entrainment at which the giver

is present, such as the occasional meal or sporting event; gifts from family or friends with whom the employees have a non-business relationship.

In any case, if employees have a question or doubt about the legitimacy of accepting an invitation or a gift, before accepting it, they should discuss the matter with General Administration Department.

1.3 Risky Activities pursuant to Legislative Decree no. 231/01 and main methods of committing offences

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with the Public Administration is generally higher concern the following:

1. Banking Supervisory Authorities relationship
2. Public Administration relationship
3. Staff selection, recruitment and management
4. Management of gifts
5. Customer relationships
6. Customer account management and monitoring
7. Credit-related activities
8. Management of payments
9. Procurement of goods and services and appointment of professional assignments
10. Management of litigation and out-of-court procedures
11. Data and Information Systems Management
12. Accounting
13. Managing relations with Business Partners and Financial Intermediaries
14. Occupational Health and Safety Management
15. Tax management
16. Marketing and sales strategies

1.3.1 Banking Supervisory Authorities relationship

The Branch's Structures are involved in the management of relations with the Supervisory Authorities and concerns all the types of activities implemented in respect of remarks, requirements, communications (including any tax verification on customers too), requests and inspections.

This Risk Activity concerns processes related to:

a) processing/transmission of occasional or periodic reports to the Supervisory Authorities;
b) requests/applications for licenses and/or authorisations;
c) feedback and compliance with applications/requests from the Supervisory Authorities;
d) management of relations with the Officials of the Supervisory Authorities during their

inspection visits;

e) monitoring remediation actions and reporting/informing the Supervisory Authority.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery and Incitement to bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis of the Criminal Code)
- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)
- Computer fraud (art. 640-ter of the Criminal Code)

By way of example, the mentioned crime could arise when the Senior persons and / or the persons subject to the management or supervision of one of the senior persons, offer or promise money or other benefits in favor of public officials or persons in charge of public service in order to perform acts that are compliant or contrary to their duties ex officio (eg. not detect irregularities that emerged during the inspection, accelerate current practices, etc.), also in case of, or subsequently to, any tax verification and/or specific data and/or documentation request made by the tax Authority in relation to both (a) the Branch; and (b) customers of the Branch, regarding information that are relevant as Predicated Offence (of Tax Predicated Offences too).

The Branch, in order to have findings omitted during the inspection represents facts different from the actual ones, or in order to have the inspection concluded expeditiously or to obtain other advantages, such as, for example, that of being informed in advance of any surprise inspections, could offer or promise undue benefits to a Public Official/Public Service Officer, even at the latter's solicitation in abuse of the exercise of its power.

The Branch could engage in artifice or deception consisting in the transmission of altered, or untrue, data, information and documents to the competent authorities in order to avoid sanctions or other measures against the Branch.

The Branch could offer or promise undue money or other benefits to an "intermediary" person, such as a consultant or a Finance Police officer, who has or asserts relationships with a Public Official or Public Service Officer in charge of conducting inspections, as the price of his or her unlawful mediation with the Public Official/Public Service Officer, in order to pursue an interest of the Branch, such as the successful outcome of the inspections and the failure of the Branch to detect infractions.

The Branch could abusively break into or damage/destroy an information or computer system protected by security measures, for example, to hide illicit acts committed by the Branch or otherwise for the Branch's benefit.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- Procedure for management of external inspections
- Suspicious transaction reporting procedure
- AnaCredit Reporting Procedure
- Conflict of interest Policy
- Operating Expense Management Rules
- AUI and SARA reporting procedure
- CRS procedure
- FATCA procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

- The contents of these protocols are aimed at ensuring that the Branch complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in handling relations with the Supervisory Authorities, including:
- the Bank of Italy
- Consob
- Data Protection Authority

1.3.2 Public Administration relationship

This Risk Activity concerns the management of relations with the Public Administration in order to fulfill obligations under laws, regulations or dispositions.

The main related processes concern:

a) management of relations with Chambers of Commerce
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding hygiene and safety and/or authorisations, permits, concessions
d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;

e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police, Guardia di Finanza);
h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g., INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to corruption (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322 and 322-bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)
- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Computer fraud (art. 640-ter of the Criminal Code)

By way of example, this offence hypothesis could take shape through the promise or payment/offer of sums of money, gifts or free benefits (outside the scope of practices concerning courtesy gifts of modest value) and the granting of advantages or other benefits of any kind - directly or indirectly, on one's own behalf or on behalf of third parties - in favor of Public Officials or public service officers, so that they perform undue acts or acts contrary to their official duties (e.g. expedite current paperwork, etc.), in order to promote or favor the interests of the Branch.
The Branch, in order to have findings omitted during the inspection represents facts different from the actual ones, or in order to have the inspection concluded expeditiously or to obtain other advantages, such as, for example, that of being informed in advance of any surprise inspections, could offer or promise undue benefits to a Public Official/Public Service Officer, even at the latter's solicitation in abuse of the exercise of its power.
The Branch could engage in artifice or deception consisting in the transmission of altered, or untrue, data, information and documents to the competent authorities in order to avoid sanctions or other measures against the Branch.
The Branch could offer or promise undue money or other benefits to an "intermediary" person, such as a consultant or a Finance Police officer, who has or asserts relationships with a Public Official or Public Service Officer in charge of conducting inspections, as the price of his or her illicit mediation

with the Public Official/Public Service Officer, in order to pursue an interest of the Branch, such as the successful outcome of the inspections and the non-detection of infractions by the Branch.
The Branch could abusively break into or damage/destroy an information or computer system protected by security measures, for example, to hide illicit acts committed by the Branch or otherwise for the Branch's benefit.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- Financial Crime Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Third-party Management Procedure
- Gifts and Entertainment Policy
- General Governance Policy of ICBC Milan Branch
- Training Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

The contents of these protocols are aimed at ensuring that the Branch complies with the current legislation and the principles of transparency, correctness, objectivity and traceability in handling relations with the Public Administration.

1.3.3 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;

j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

Non-transparent management of the staff selection and recruitment process could allow the commission of such offences through the promise of hiring made to representatives of the Public Administration and/or senior officers and/or their staff in companies or entities that are counterparties or in relationships with the Branch, or to persons indicated by them, in order to influence their independence of judgment or to ensure any benefit for the Branch.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Embezzlement (Article 314 of the Criminal Code 1st paragraph)
- Embezzlement takin profit from other's mistake (Article 316 of the Criminal Code)
- Bribery and incitement to bribery (Article 318, 319 quater, 322, 323 of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the mentioned crime could be configured in the case of the realization of one of the following conducts: improper management of assumptions, with the aim of privileging persons reported by public officials or persons in charge of a public service and therefore constituting the usefulness guaranteed to the latter in the context of the crime of corruption; or improper management of the definition of remuneration policies, if the remuneration is the preordained means by which the Senior person and / or the persons subject to the management or supervision of one of the Senior persons of the Branch could bribe the public official or the person in charge of a public service, undue improvement of an employee's working conditions as connected with (or otherwise reported by) public officials or persons in charge of public service..

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- HR Management System Instructions March 2023
- Measures Staff Recruitment
- Performance Appraisal Guidelines
- Gifts and Entertainment Policy

- Code of Ethics
- Code of Conduct
- Staff Handbook
- Third-party Management Procedure
- Conflict of interest Policy
- Anti-Internal Fraud Policy
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Employer Personal Data Processing Policy
- Rights and duties of the employees disciplinary measures
- Operating Expense Management Rules
- Whistleblowing Policy
- Training Policy

1.3.4 Management of gifts

Employees shall not receive or give gratuities or benefits in whatever form that might give rise to a conflict of interests with respect to obligations towards the clients or be in contravention of the Branch's Code of Conduct or non-coherence with the provisions of the Gifts and Entertainment Policy and Anti-Bribery and Anti-Corruption Policy. Employees must obtain pre-approval General Administration Department prior to accepting gifts or entertainments valued above €100. Approval must be obtained from the General Management if the gifts or benefits are addressed to a member of the General Administration Department. In case gifts or benefits are addressed to the General Administration Department, the necessary approval must be obtained from the General Management. The offering and receiving of reasonable business entertainment may fall outside these requirements.

This Risk Activity mainly concerns processes related to:

a) Management of liberal initiatives;
b) Management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the promise or payment/offer of undue sums of money, free gifts or benefits (outside the scope of practices relating to courtesy gifts of modest value) and the granting - directly or indirectly, on one's own behalf or on behalf of third parties - of advantages or other benefits of any kind to representatives of the Public Administration in order to promote or favour the interests of the Branch could constitute the offence of corruption.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Centralized Procurement Rules
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.5 Customer relationships

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery and incitement to bribery (Articles 318, 319, 319 ter, 319 quater, 320, 320, 321, 322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the offenses under consideration may exist if the Senior persons and / or persons subject to the management or supervision of one of the senior persons, offer or promise money or other benefits to public officials or public service officers to work against their official duties (for example to don't detect irregularities that emerged during the inspection in relation to customer relations and account information and anti-money laundering compliance, to speed up current practices in customer relations, etc.).

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- PEP Procedure
- Financial Crime Policy
- Customer Due Diligence Archiving Procedure
- BRAINS Manual
- CIB Business Manual
- Banking Business Manual
- DAC-6 procedure
- CRS procedure
- Credit Manual;
- FATCA Procedure
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Tax Affair Management Procedure
- Code of Ethics
- Code of Conduct
- Staff Handbook
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- Anti-Internal Fraud Policy
- General Governance Policy of ICBC Milan Branch

- Complaint handling Procedure
- Whistleblowing Policy
- Measures Staff Recruitment
- Operating Expense Management Rules
- Third-party Management Procedure

1.3.6 Customer account management and monitoring

This Risk Activity concerns processes related to:

a) customer account profile management
b) account opening/closing;
c) management of dormant customers, dormant accounts and possible re-activation;
d) deviations from standard tariffs;
e) monitoring of accounts and customer information;
f) RMA exchange operation with the correspondent bank;
g) management of account or other product usage anomalies.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Computer fraud (Article 640-ter of the Criminal Code)

By way of example, the crime in question could occur in the event that The Branch, in the context of customer account management, implements artifice or deception consisting in the transmission of altered, or untrue, data, information and documents to the competent authorities in order to avoid sanctions or other measures against The Branch.
The Branch could abusively break into a computer or telematic system protected by security measures or damage/destroy an information system, for example, in order to hide illicit acts committed by the Branch or otherwise for its benefit.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- BRAINS Manual
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure

- Credit Manual
- Anti Internal Fraud Policy
- Banking business manual
- Charter of Credit Committee
- Conflict of interest Policy
- General Governance Policy of ICBC Milan Branch
- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- Suspicious Transaction Reporting Procedure
- Whistleblowing Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.7 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;
c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Computer fraud (Article 640-ter of the Criminal Code)

By way of example, the offence in question could occur in the context of the activities described above relating to the processes connected to the granting of credit, in the event the Branch carries out artifices or deception consisting in the transmission of altered or untrue data, information and documents to the competent authorities, in order to avoid sanctions or other measures against the Branch.

The Branch could omit verification activities functional to the granting of credit not in line with the company policies in favour of a subject related to a public official in order to obtain an advantage for the Branch or could prepare or update appraisals in order to favour subjects favourable/close to a

public official/related to the Public Administration (e.g. avoid detection and consequent payment of sanctions during inspections by Public Administration officials).
The Branch may also abusively enter a computer or telematic system protected by security measures or damage/destroy an information system, e.g. in order to conceal offences committed by the Branch or otherwise to its advantage.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- Financial Crime Policy
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Credit Manual
- Anti Internal Fraud Policy
- Banking Business Manual
- Charter of Credit Committee
- CIB Business Manual
- Complaint handling procedure
- Conflict of interest Policy
- CRS procedure
- Dac-6 procedure
- Financial Accounting Manual
- General Governance Policy of ICBC Milan Branch
- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- Market Abuse Policy
- Procedure for Assessment and Approval of New Product
- Suspicious Transaction Reporting procedure
- Tax Affair Management Procedure
- Treasury manual
- Whistleblowing Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.8 Management of payments

This Risk Activity concerns processes related to the management of the payment of sales/goods/services actually rendered/received.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the offense could take place in the event that part of the salary is paid to employees in the form of reimbursement, in order to avoid the payment of part of the contributions due to the public institutions.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Operating Expense Management Rules
- Internal Operation and Management Authorization
- Banking Business Manual
- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Financial Crime Policy
- Gifts and Entertainment Policy
- Suspicious Transaction Reporting Procedure
- Third-party Management Procedure
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Internal Fraud Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.9 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;

b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319-ter, 319-quater, 320, 320, 321, 322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the crime of bribery could occur in the event that an employee of the Branch offers goods, money or other illicit benefits to suppliers that have or allege relationships with members of the Public Administration, as the price of the latter's illicit mediation with the Public Administration in order to pursue an interest of the Branch such as in obtain goods / services at better sales conditions and / or at more favorable prices.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- Third-party Management Procedure
- Centralized Procurement Rules
- Policy on the Management of the External Legal Advisors
- Gifts and Entertainment Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Operating Expense Management Rules
- Financial Crime Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Conflict of interest Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct

- Staff Handbook

1.3.10 Management of litigation and out-of court procedures

This Risky Activity concerns activities related to all the Branch Structures involved in the:

a) complaints management;
b) management of active and passive judicial/out-of-court disputes (civil, criminal, administrative, labour law - debt collection) also with the external professional's assistance;
c) managing and monitoring settlement agreements.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319 ter, 319 quater, 320, 321,322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the offence of bribery could be committed where an employee offers money, goods or other benefits to an intermediary who has or claims to have relations with a Public Official or person in charge of a Public Service as the price for his illicit mediation with the latter in order to procure an undue benefit to the Branch.
The Branch, in order to obtain undue advantages in a judicial/ extrajudicial proceeding in which it is involved, could assign files to external professionals through whom it could carry out corruptive activities towards the judicial authority or select external professionals close or connected, directly or indirectly, to the Public Administration, in order to obtain undue advantages in a judicial proceeding.
The Branch could offer or promise benefits to a magistrate or to a member of an arbitration board, also through the intermediary of the external professional appointed by the Branch, in order to obtain a favourable judgement in court and/or to know the orientation of the magistrate or of the arbitrator in advance of the publication of the decision.
The Branch may offer or promise benefits to a Public Official/Person in charge of a Public Service, acting as a representative of the counterparty in a judicial/ extrajudicial litigation, in order to reach a settlement agreement more favorable.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Policy on the Management of External Legal Advisor
- Anti-Bribery and Corruption Policy

- Complaint handling Procedure
- Legal function working manual
- Third-party Management Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti Internal Fraud Policy
- Code of Ethics
- Code of Code of Conduct
- Staff Handbook

1.3.11 Data and Information Systems Management

This Risk Activity concerns processes related to:

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;
b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Computer fraud (art. 640-ter of the Criminal Code)

By way of example, such offences could occur if the Branch abusively breaks into a computer or telematic system protected by security measures or damages/destroys an information system, for instance, in order to hide illicit acts committed by the Branch or otherwise to its advantage.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Guidelines on System and Network Management

- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- ICBC (Europe) S.A. Milan Branch Employer Personal Data Policy
- ICBC (Europe) S.A. Data Retention Policy
- ICBC (Europe) S.A. Rules of Privacy by Design and Privacy by Default
- ICBC Privacy policy
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Rules of IT General Management
- Information Security Policy
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- IT Governance-Equipment Management
- Measures of Information and Information System Security Management
- Milan Branch Employer Personal Data Processing Policy
- Power of attorney Branch to HQ data transfers GDPR
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- Security Management-Network&System Security
- Social Media Policy
- Technical Specifications for Security Technique for Network System
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.12 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;
c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;

f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Headquarter.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319 quater, 320, 321,322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the type of offence in question could occur where the Branch could promise or give sums of money or other benefits not due to the Public Official or Person in Charge of a Public Service deriving from the recording in the Bank's accounts (in relation to suppliers and customers), of management facts that do not correspond to the truth, in order to create extra-accounting funds to be used for corrupt purposes.

With specific regard to the management of the recovery of bad debts and related loss forecasts, the Branch could engage in artifice or deception towards public entities aimed at representing a higher credit than the actual one.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- Third Party Management
- Financial Accounting Manual
- Credit Manual
- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Anti Internal Fraud Policy
- Code of Ethics
- Code of Conduct

- Staff Handbook

1.3.13 Managing relations with Business Partners and Financial Intermediaries

This Risk Activity concerns processes related to:

a) identification and selection of business partners;
b) monitoring the situation of similar local banks;
c) preparation, organisation and execution of the marketing plan.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319 quater, 320, 321,322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the type of offence in question could arise where the Branch, as a result of negotiating with business partners/financial intermediaries fictitious commissions or commissions in excess of what is actually due for the services rendered, could create extra-accounting funds to be used for corrupt purposes.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Credit Manual
- Banking Business Manual
- General Governance Policy of ICBC Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure
- Operating Expense Management Rules
- Whistleblowing Policy
- Conflict of interest Policy
- Internal Operation and Management Authorization
- Complaint handling procedure
- Conflict of interest Policy
- International Settlement and Trade Finance Operation Manual
- Gifts and Entertainment Policy
- Anti Internal Fraud Policy

- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.14 Occupational Health and Safety Management

This Risk Activity concerns processes related to compliance with any type of activity aimed at developing and ensuring a system of prevention and protection of workplace risks, in compliance with the provisions of Legislative Decree No. 81/2008 as amended:

a) organisation of roles and activities related to the protection of Health and Safety at Work;
b) management of risk assessment activities and preparation of the consequent prevention and protection measures;
c) management of emergencies;
d) information, training and involvement of workers in occupational Health and Safety;
e) management of health surveillance;
f) detection, recording and management of accidents and incidents.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319 quater, 320, 321,322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, this type of offence could occur if a Branch employee offers money or other benefits to Public Officials or Persons in Charge of a Public Service so that they do not detect irregularities in the correct application of the rules on Health and Safety at Work.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct
- DVR - Documento sulla Valutazione dei Rischi
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Staff Handbook

1.3.15 Tax management

This Risk Activity concerns processes related to:

a) drafting, approving and sending tax declarations or payment forms;
b) direct and indirect taxes payments;
c) management of active/passive invoicing;
d) storage of accounting records.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)
- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)

By way of example, the type of offence in question could occur in the event the Branch carries out artifices or deception such as, for example, the falsification of documents in tax matters, also in conspiracy with other persons, such as to induce the Public Administration into error, in order to obtain an unfair profit to the detriment of the same, or if they offer or promise money or other undue utility to a Public Official or Person in Charge of a Public Service during a procedure aimed at verifying compliance with the requirements imposed or an inspection.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct
- Anti-Bribery and Corruption Policy
- Tax Affairs Management Procedure
- Financial Accounting Manual
- Treasury Manual
- Internal Operation and Management Authorization
- General Governance Policy
- Whistleblowing Policy
- Staff Handbook

- Conflict of interest Policy
- Credit Manual
- Dac-6 procedure
- CRS Procedure
- FATCA Procedure
- Suspicious Transaction Reporting procedure.
- Anti Internal Fraud Policy

1.3.16 Marketing and sales strategies

This Risk Activity concerns processes related to:

a) promotion of the Branch's image on the Italian market;
b) development of marketing and sales strategies;
c) management of relations with prospects;
d) organisation of meetings with potential clients;
e) management of external reporting;
f) management of the proposition of new products, services or activities of the Branch (Definition of business needs; Preliminary investigation and evaluation of new products/services; Approval of new products/services).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Corruption and incitement to bribery (Articles 318, 319, 319 quater, 320, 321,322 e 322 bis of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the offences in question could occur where the Branch offers or promises undue money or other benefits to a Public Official or Person in Charge of a Public Service in order not to reveal during an inspection procedure that it has put on the market banking products with characteristics other than those declared and approved following the internal evaluation processes of the new product/service.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Banking Business Manual;

- Procedure for Assessment and Approval of New Product
- Financial Accounting Manual
- ICBC Milan Branch Business Processing Procedures of Financial Markets Business
- ICBC EUROPE S.A. Milan Branch Administrative Measures for Financial Markets Business Internal Operation and Management Authorization
- Responsibilities of Financial Accounting & IT Department
- Centralized Procurement Rules
- Treasury manual
- Dac-6 procedure
- CRS procedure
- Procedure on the management of external legal advisors
- Financial Crime Policy
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Tax Affair Management Procedure

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. identification of the persons in charge of providing suitable and appropriate documentation in response to requests by the Supervisory Authority and the Public Administration;
2. implementation of all the organisational-accounting measures necessary to extract the data and information for the correct compilation of the reports and their timely submission to the Supervisory Authority, in accordance with the procedures and timescales established by the applicable legislation;
3. traceability of relations with the officials of the Supervisory Authority and the Public Administration for the performance of fulfilments connected to the Branch activity and/or following audits/inspections;
4. filing and preservation of the documentation produced;
5. controls of completeness, correctness and accuracy of the information transmitted by each department to the Supervisory Authorities and to the Public Administration;
6. management in a transparent and unambiguous manner of any professional relationship established with members of the Public Administration or with persons qualifying as Public Officials or persons in charge of a public service;
7. definition of rules to be followed when receiving gifts and gratuities in the area of relations with members of the Public Administration;
8. transparency and integrity of the Branch in its business relations in order to avoid any

improper advantage;

9. transparent and reconstructible decision-making processes over time concerning the conditions stipulated with customers;
10. definition of the methods and criteria underlying any amendments and/or renewals of the conditions stipulated with customers;
11. definition of controls on potentially anomalous transactions, in terms of amount, type, object or frequency including to check if the amount, type, receiver, purpose of the payment are consistent with the approved payment application before effectuating the payment, and to archive the related documents to ensure traceability afterwards;
12. accurate verification of the necessary qualifications, skills and requirements of suppliers;
13. adequately formalised requests for tenders addressed to suppliers;
14. traceability of access and critical activities carried out through the Branch's IT systems;
15. traceability of all IT events, problems and changes to the Branch's IT system;
16. provision of procedures for reporting any omissions, tampering, falsifications or negligence in the accounts or supporting documentation on which accounting records are based;
17. checks on the completeness, correctness and accuracy of the documentation and information supporting the determination and related payments of direct and indirect taxes;
18. monitoring the deadlines for preparing and sending tax documentation;
19. checking the compliance of the characteristics and operation of new products/services with applicable regulations and internal rules;
20. de-activation of user credentials for staff who have lost the right to access computer systems at the end of their employment or individual activity.
21. periodical monitoring/control activities on the branch operations also by the Surveillance Body;
22. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
23. staff awareness activities in the areas of the Branch's operations.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Articles 24 and 25 of the Decree "Offences against the Public Administration", the following should be noted:

1. Branch employees shall immediately report to their Head any suspected act of corruption by a Public Administration official of which they may be the recipient or simply become aware;
2. no payments may be made to Public Administration officials in order to ensure or expedite a routine task by a Public Official;
3. the staff recruitment and employment process must be motivated by actual business needs and based on criteria that are non-arbitrary and as objective as possible;
4. in the staff recruitment and employment process, the best candidate is selected on the basis

of merit and not on the basis of external connections; checks are carried out to ensure that the candidate has no relationship with public officials (national or foreign) and that the recruitment practices have not been conducted in a situation of conflict of interest;

5. no gifts of money, even for business purposes, are to be accepted (cash, cheques, gift cards, etc.);
6. any exception to the Gifts and Entertainment Policy may only be made if approved by the General Administration Department (or the General Management if a member of the General Administration Department is involved in the gift in question);
7. all documentation produced, relating to the execution of the fulfilments carried out within the framework of the management of gifts, gratuities, sponsorships, entertainment expenses and charities is filed by the General Administration Department in a "Gift Tracking Table" which contains:
    - a brief description of the gift
    - the name of the person making the gift and the name of the recipient;
    - the estimated value of the gift;
    - whether the gift was accepted or refused and what its final destination was;
    - any exceptions to the Internal Policies, duly justified.
8. when establishing a relationship with a potential supplier or any review of an existing contractual relationship, in order to assess the corruption risk of each supplier, the relevant Department shall carry out due diligence/Know Your Supplier activities. Indicators of corruption risk for suppliers, such as the supplier's ethical standards, the supplier's economic dependence on the Branch or the Branch's dependence on the supplier, shall be considered;
9. contracts with suppliers contain specific contractual clauses providing for the supplier's commitment to comply with applicable laws.

SECOND SECTION - COMPUTER CRIMES AND UNLAWFUL DATA PROCESSING

1.1. Introduction

The Article 24-*bis* of the Legislative Decree no. 231/2001 lists the series of computer crimes which might give rise to the administrative liability of Entities.

The crimes provided for in this article are aimed to combat the spread of cybercrime directed against the confidentiality, integrity and availability of computer systems, network and data. In addition, the crimes concern the protection of personal data, essentially in order to facilitate investigations of computer data and allow for the preservation of internet traffic data for certain periods.

In order to better understand the provisions contained in the aforementioned article, the following

definitions are taken into consideration:

- “computer system” means: any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- “computer data” means: any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

Specifically, Computer crimes, set out in Article 24-bis of the Decree, include:

- **Unauthorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)**: this offence is committed by anyone who illegally enters a computer or telecommunication system protected by security measures or remains in it against the express or tacit will of the person entitled to exclude him.
- **Unauthorized possession and distribution of computer or telecommunication systems’ access codes (Art. 615-quater Criminal Code)**: this offence is committed by anyone who, in order to procure a profit for himself or others or to cause damage to others, unlawfully obtains, holds, produces, reproduces, disseminates, imports, communicates, delivers, otherwise makes available to others or installs equipment, instruments, parts of equipment or instruments, codes, passwords or other means of accessing a computer or telecommunications system protected by security measures, or in any case provides indications or instructions suitable for that purpose.
- **Distribution of computer equipment, devices or computer programs for the purpose of damaging or interrupting a computer or a telecommunication system’s operations (Art. 615-quinquies of the Criminal Code)**: this offence is committed by anyone who, with the aim of unlawfully damaging a computer or telecommunications system, the information, data or programmes contained therein or pertaining thereto, or of favouring the total or partial interruption or disruption of its operation, unlawfully obtains, possesses, produces, reproduces, imports, disseminates, communicates, delivers or, in any other way, makes available to others or installs computer equipment, devices or programmes.
- **Illegal interception, obstruction or interruption of computer or telematic communications (Article 617-quater of the Criminal Code)**: this offence is committed by any person who fraudulently intercepts communications relating to a computer or telematic system or between several systems, or obstructs or interrupts them, or, unless the fact constitutes a more serious offence, discloses to the public, by any means, the whole or part of the content of such communications.
- **Installation of devices aimed at wiretapping, blocking or interrupting computer or information technologies communications (Article 617-quinquies of the Criminal Code)**: this offence is committed by anyone who, except in cases permitted by law, procures,

possesses, produces, reproduces, disseminates, imports, communicates, delivers, otherwise makes available to others or installs equipment, programmes, codes, passwords or other means designed to intercept, prevent or interrupt communications relating to a computer or telecommunications system or between several systems, or to prevent or interrupt them.

- **Damaging computer information, data and programs (Art. 635-bis of the Criminal Code)**: unless the offence constitutes a more serious offence, anyone who destroys, deteriorates, deletes, alters or suppresses the computer information, data or programmes of others shall be liable for this offence.
- **Damaging computer information, data and programs used by the Government or any other public Entity or by an Entity providing public services (Art. 635-ter of the Criminal Code)**: unless the act constitutes a more serious offence, anyone who commits an act aimed at destroying, deteriorating, deleting, altering or suppressing computer information, data or programmes used by the State or another public body or pertaining to them, or in any case of public utility, shall be liable for this offence.
- **Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)**: unless the act constitutes a more serious offence, anyone who, by means of the conduct referred to in Article 635-bis, or by introducing or transmitting data, information or programmes, destroys, damages, renders wholly or partially unusable computer or telecommunication systems of others or seriously obstructs their operation.
- **Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)**: anyone who commits the offence referred to in Article 635-quater in order to render computer or telecommunication systems of public utility useless or to seriously obstruct their operation shall be liable for this offence.
- **Computer fraud by the electronic signature certifier (Art. 640-quinquies of the Criminal Code)**: this offence is committed by any person who provides electronic signature certification services and who, in order to procure an unfair profit for himself or others or to cause damage to others, violates the obligations laid down by law for the issuance of a qualified certificate.
- **Violation of the rules on the National Cyber Security Perimeter (Article 1, paragraph 11, Decree-Law No. 105 of 21 September 2019)**: anyone who, with the aim of hindering or conditioning the Authorities in charge of protecting the strategic technological infrastructure system, provides untrue information, data or factual elements relevant:
  a) for the preparation and updating of lists of the networks, systems (including their architecture and components) and IT services of the Public Administration and of public and private operators based in Italy, on which the exercise of an essential function of the State or the provision of a service essential for fundamental civil, social or economic activities depends and, on the malfunctioning, interruption or abuse of which a danger to

national security may arise;

b) for the purposes of the notifications that said public and private operators must make to the National Assessment and Certification Centre (CVCN) established at the Ministry of Economic Development of the supply contracts that they intend to enter into to procure ICT goods, systems and services to be used in the networks, systems and services referred to in the preceding point

c) for the performance of inspection and surveillance activities concerning compliance with the provisions and procedures relating to the preparation and updating of lists, notification of supplies and notification of incidents and security measures relating to systems, networks and services, or fails to communicate data, information or facts within the required time limit.

- **Computerised documents (Article 491-bis of the Criminal Code)**: this Article provides that the same criminal provisions provided for in Articles 476 to 493 of the Criminal Code (offences of material or ideological falsity, falsity in registers and notifications, use of false documents) apply to public computerised documents having evidentiary effect.

1.2. General rules of conduct

The purpose of the following general rules of conduct is that all Recipients of the Model adopt strict rules of behavior in order to prevent the commission of offences provided in Article 24-bis of Legislative Decree no. 231/01.

Each employee is directly responsible for goods entrusted by the Branch in order to perform the assigned tasks, in particular the employee must guarantee the protection and conservation of the aforementioned goods and use it in compliance with the rules provided for conservation and protection.

Employees must pay attention and care in the management of the instruments, whatever the technological nature, and the information; for example, when sending e-mails, in the internet connection, the use of the telephone, e-mail, etc., their use must always be reasonably limited to purposes strictly related to the Branch's activity.

Goods refer not only to the material instruments provided to support the activities, but also to any other intangible asset (data, information, procedures) that the Branch assigns to its employees in order to facilitate and allow a better realization of its tasks and its objectives.

The information acquired in carrying out the activities of the Branch must remain strictly confidential and appropriately protected and may not be used, communicated or disclosed within and outside the Branch, except as required by current legislation and Branch procedures.

The following categories of data must be treated with caution and confidentiality:

- proprietary information of the Branch, included any system, information or process that gives the branch an opportunity to obtain an advantage over our competitors, nonpublic information about the Branch's operations, results, strategies and projections, non-public information

about the Branch's business plan, business processes and client relationship, non-public employee information, non-public and other confidential information received in the course of the employment about costumers and potential costumer, suppliers/subcontractors and distributors, non-public information about the Branch's technology system and proprietary products.

- customer's personal data, including biographical data, health data and news or information regarding their financial situation, experience in investments in financial instruments, investment objectives, risk appetite.
- employee's personal data, including biographical data and health data
- any other news, data, information of a confidential nature concerning customers and the Branch.

The Branch adopts and updates specific procedures aimed at protecting information in accordance with the General Data Protection Regulation (GDPR). In particular, the Branch:

- ensures the correct separation of roles and responsibilities within the various figures in charge of processing information;
- signing specific agreements, including confidentiality, with third parties that are involved in information processing, or which in any way may come into possession of confidential information.

All Recipients of this Model, with reference to any information learned on account of their work functions, are obliged to ensure maximum confidentiality, also in order to safeguard the technical, financial, legal, administrative, managerial and commercial know-how of the Branch.

In particular, each employee must:

- acquire and process only the information and data necessary for the purposes of its department;
- acquire and process information and data only within the limits established by the procedures adopted by the Branch;
- keep the data and information in order to prevent its spread among unauthorized persons;
- communicate and disclose data and information, inside and outside the Branch, only to parties who have an effective and justified need to know them for work purposes and, in general, in compliance with the procedures adopted by the Branch;
- observe the obligation of confidentiality even after termination of the relationship with the Branch, in accordance with local regulations and / or contractual obligations.

The Branch is committed to protecting the privacy of all information of any kind or object which comes into possession in carrying out its activities, avoiding any misuse or improper circulation of such information.

The circulation of information within the Branch must be accompanied by specific cautions and warnings and it is therefore necessary:

- make sure that the personal computer, where confidential documents are stored, are protected by passwords;
- keep confidential documents in a safe or in locked cabinets by the manager of the organizational unit for as long as necessary to avoid improper use;
- not to bring outside the Branch confidential documents;
- use the appropriate document shredders for the confidential material to be removed;
- keep confidential information concerning the Branch, its customers and business partners, its organization and the internal regulations governing its operation;
- even when discussing among colleagues, refraining from mentioning names, operations and figures in public places, which could be heard by extraneous listeners.

In particular, the Branch on the use of electronic goods provides that only the Financial Accounting & IT Department can make copies of software, for back-up or security purposes.

All employees must ensure that no unlawful copies are made or used on the branch's premises.

Installation of any software on computers connected to the network must be carried out by the members of IT staff, or with prior consent from Financial Accounting & IT Department, it can be carried out by software supplier with the attendance of IT staff. Other staffs are not allowed to install any application by themselves.

In addition, the employees must:

- do not use any unauthorized discs, for example computer games;
- does not purchase, without authorization, copies of PC software for your use at the Branch;
- contact the Financial Accounting & IT Department if the PC shows symptoms of having a virus;
- observe the requirements of the Branch with respect to computers and the Internet as they may be amended from time to time.

1.3 Risky activities pursuant to Legislative Decree no. 231/01 and main methods of committing offences

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Computer Crimes is generally higher concern the following:

1. Banking Supervisory Authorities relationship
2. Public Administration relationship
3. Procurement of goods and services and appointment of professional assignments
4. Management of payments
5. Staff selection, recruitment and management
6. Data and Information Systems Management
7. Accounting

1.3.1 Banking Supervisory Authorities relationship

This Risk Activity concerns processes related to:

a) processing/transmission of occasional or periodic reports to the Supervisory Authorities;
b) requests/applications for licenses and/or authorisations;
c) feedback and compliance with applications/requests from the Supervisory Authorities;
d) management of relations with the Officials of the Supervisory Authorities during their inspection visits;
e) monitoring remediation actions and reporting/informing the Supervisory Authority.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Unauthorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)
- Damaging computer information, data and programs (Article 635-bis of the Criminal Code)
- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

By way of example, the offence could be committed if the Recipients of the Model anomalously manage applications constituting potential support for the commission of the offence of computer fraud or swindling, allowing access, alteration and deletion of data and information intended for the Supervisory Authorities or damaging/destroying a computer system, in order to hide illicit acts committed or to gain an advantage.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- AUI and SARA reporting procedure
- CRS procedure
- FATCA procedure

- Procedure for management of external inspections
- Suspicious transaction reporting procedure
- AnaCredit Reporting Procedure
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Public Administration relationship

This Risk Activity concerns processes related to:

a) management of relations with Chambers of Commerce;
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding hygiene and safety and/or authorisations, permits, concessions;
d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;
e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office ;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police, Guardia di Finanza);
h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g. INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Unauthorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)
- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

By way of example, the offence could be committed if the Recipients of the Model anomalously

manage applications constituting potential support for the commission of the offence of computer fraud or swindling, allowing access, alteration and deletion of data and information intended for the Public Administration or damaging/destroying a computer system, in order to hide illicit acts committed or to gain an advantage.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- General Governance Policy of ICBC Milan Branch
- Financial Crime Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Training Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.3 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Unauthorised access to a telecommunications or computer system (Article 615-ter of

the Criminal Code)

- Damaging computer information, data and programs (Article 635-bis of the Criminal Code)
- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

By way of example, the offence could be committed in the event that a Branch employee unlawfully breaks into a Branch computer or electronic system in order to destroy, deteriorate, delete, alter or suppress information, data relating to relations with suppliers/consultants/external professionals from which a legal liability of the Branch could arise.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Third-party Management Procedure
- Policy on the Management of the External Legal Advisors
- Centralized Procurement Rules
- General Governance Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Financial Crime Policy
- Internal Operation and Management Authorization
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.4 Management of payments

This Risk Activity concerns processes related to the management of the payment of sales/goods/services actually rendered/received.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Unauthorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)
- Unauthorized possession and distribution of computer or telecommunication systems' access codes (Article 615-quater of the Criminal Code)
- Distribution of computer equipment, devices or computer programs for the purpose of damaging or interrupting a computer or a telecommunication system's operations (Article 615-quinquies of the Criminal Code)
- Wiretapping, blocking or illegally interrupting computer or information technology communications (Article 617-quater of the Criminal Code)
- Installation of devices aimed at wiretapping, blocking or interrupting computer or information technologies communications (Article 617-quinquies of the Criminal Code)
- Damaging computer information, data and programs (Article 635-bis of the Criminal Code)
- Damaging computer information, data and programs used by the Government or any other public Entity or by an Entity providing public services (Article 635-ter of the Criminal Code)
- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

By way of example, the crime could take place in the event that the employee doesn't proceed with the correct registration of invoices or he introduces into the computer system to modify the stored data.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Operating Expense Management Rules
- Financial Crime Policy
- Banking business manual
- Suspicious Transaction Reporting Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Centralized Procurement Rules

- Third-party Management Procedure
- Anti Internal Fraud Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.5 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Unauthorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)
- Damaging computer information, data and programs (Article 635-bis of the Criminal Code)
- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

By way of example, the offence could occur if the Branch, in preparing, approving and sending tax, insurance and contribution declarations, commits a falsehood concerning a public and/or private electronic document with probatory value.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- HR Management System Instructions March 2023
- Measures Staff Recruitment
- Operating Expense Management Rules
- Employer Personal Data Processing Policy
- Rights and duties of the employees disciplinary measures
- Code of Ethics
- Code of Conduct
- Staff Handbook
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Third-party Management Procedure
- Performance Appraisal Guidelines
- Training Policy

1.3.6 Data and Information Systems Management

This Risk Activity concerns processes related to:

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;
b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)
- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Un-authorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)
- Unauthorized possession and distribution of computer or telecommunication systems' access codes (Article 615-quater of the Criminal Code)
- Distribution of computer equipment, devices or computer programs for the purpose of damaging or interrupting a computer or a telecommunication system's operations (Article 615-quinquies of the Criminal Code)
- Wiretapping, blocking or illegally interrupting computer or information technology communications (Article 617-quater of the Criminal Code)
- Installation of devices aimed at wiretapping, blocking or interrupting computer or information technologies communications (Article 617-quinquies of the Criminal Code)
- Damaging computer information, data and programs (Article 635-bis of the Criminal Code)
- Damaging computer information, data and programs used by the Government or any other public Entity or by an Entity providing public services (Article 635-ter of the Criminal Code)

By way of example, such offences could be committed in the event the Branch has not adopted the appropriate data protection measures and, therefore, employees are free to access computer systems without having received specific authorisation. In this case, from the non-adoption of appropriate preventive measures, the Branch could obtain a cost saving, configurable as an unlawful profit. Consider also the case where a Branch employee illegally accesses the customer database of a competitor in order to get hold of sensitive data and enable the Branch to obtain an unfair competitive advantage.
For the crime of damaging computer or telecommunication systems, could be punished any person who, by introducing or transmitting data, information or software, destroys, damages or makes it impossible, either in whole or in part, to use another person's computer or telecommunication system or seriously obstructs its functioning. For this offence to be committed, the system so attacked must be damaged or rendered unusable at least in part, or its functioning must be obstructed.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Measures of Information and Information System Security Management

- ICBC (Europe) S.A. Rules of IT General Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Breach Management Procedure
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- Guidelines on System and Network Management
- Technical Specifications for Security Technique for Network System
- Security Management – Network &System Security
- IT Governance-Equipment Management
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Data Retention Policy
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- ICBC (Europe) S.A. Milan Branch Employer Personal Data Policy
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A. Rules of Privacy by Design and Privacy by Default
- ICBC Privacy policy
- Milan Branch Employer Personal Data Processing Policy
- Power of attorney Branch to HQ data transfers GDPR
- Social Media Policy
- Information Security Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti Internal Fraud Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.7 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;

c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;
f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Headquarter.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Forgery of electronic documents (Article 491-bis of the Criminal Code)
- Unauthorised access to a telecommunications or computer system (Article 615-ter of the Criminal Code)
- Damaging computer information, data and programs (Article 635-bis of the Criminal Code)
- Damaging computer or telecommunication systems (Article 635-quater of the Criminal Code)
- Damaging computer or telecommunication systems of public interest (Article 635-quinquies of the Criminal Code)

By way of example, this type of offence could occur if a Branch employee illegally accesses computer systems and manipulates data in order to obtain an advantage with regard to accounting and financial statement requirements.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Financial Accounting Manual
- Credit Manual
- Anti Internal Fraud Policy
- Operating Expense Management Rules
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Gifts and Entertainment Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Third Party Management
- Code of Ethics
- Code of Conduct

- Staff Handbook

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of the persons in charge of managing data and information systems;
2. definition of univocal access credentials;
3. traceability of accesses and critical activities carried out through the Branch's IT systems;
4. deactivation of credentials associated with personnel who have lost the right to access information systems upon termination of their employment or at each single activity;
5. prompt identification of system vulnerabilities;
6. archiving and storage of the documentation concerning what each department manages in special electronic folders;
7. definition of controls on potentially anomalous transactions, in terms of amount, type, object or frequency;
8. monitoring the effectiveness and operability of the information security management system;
9. use of multi-layered firewalls to ensure the security of the Branch's website and computer system;
10. tracking of all IT events, problems and changes to the Branch's IT system;
11. provision of procedures for reporting any omissions, manipulations, falsifications or neglect of accounts or supporting documentation on which accounting records are based;
12. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
13. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
14. staff awareness activities in the areas of the Branch's operations.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 24-bis "Computer Crimes", the following should be noted:

1. the Financial Accounting & IT Department conducts audits and risk assessments in order to ensure adequate levels of IT security, IT risk management and IT compliance;
2. training and awareness-raising initiatives are carried out for staff on the correct use of IT applications and tools in terms of information security and confidentiality;
3. the Financial Accounting & IT Department develops business continuity and disaster recovery tests;
4. Head Office and Headquarter carry out periodic inspections to verify the branch's IT security systems;
5. backup systems are in place to help raise the level of protection against the loss of personal

and critical data;

6. employees promptly report potential security incidents in order to minimise damage;
7. copying of data through the use of USB sticks is not permitted for security reasons;
8. company documents are produced, copied, faxed, archived, stored and disposed of by means designed to minimise the risk of unauthorised persons gaining access to private or confidential information.

THIRD SECTION - ORGANIZED CRIME OFFENCES

1.1. Introduction

Article 24-ter of the Decree, introduced by Law no. 94/2009, concerning a group of offences relating to the various forms of criminal organizations.

With reference to the types of criminal association included in this article, the offence consists in promoting, establishing and participating in a criminal association consisting of three or more persons, and is therefore punishable per se regardless of if the crimes pursued by the association are actually committed (any such crimes being punished separately).

Consequently, the intentional participation of a representative or employee of the entity in a criminal association might of itself give rise to the entity's administrative liability, provided, of course, that participation in or support for such criminal association is also in the entity's interest or gives an advantage to it. Moreover, the association must involve at least some form of stable organisation and a common plan to carry out an indefinite series of crimes. In other words, an occasional agreement for the commission of one or more specific crimes does not constitute the offence of criminal association.

Under case law, the offence of aiding and abetting a criminal association is committed by a person who, while not being a member of such association, contributes in a significant manner, although occasionally, to its existence or to the pursuit of its objectives.

The mafia-type criminal association (Article 416-bis of the Criminal Code) differs from the generic criminal association in that its participants exploit the intimidating power of their association and the resulting condition of submission and silence to commit crimes or – even without committing crimes, yet by use of the mafia method – to directly or indirectly acquire control over economic activities, concessions, authorizations, public contracts and services, or to obtain unlawful profits or advantages for themselves or for others, or with a view to preventing or limiting the freedom of vote, or to obtain votes for themselves of for others on the occasion of an election.

This provision also applies to the 'camorra' and other criminal organizations, howsoever named, including foreign crime syndicates, possessing the above-mentioned mafia-type characteristics. It is applicable to anyone, by proceeding in causing social fear, is prosecuting illegal purposes by using

means equivalent to the Mob style (so including all conducts that cannot be classified into a specific type of organization).

The crime of vote exchange in elections is committed by a person who proposes or accepts the promise to procure votes with the use of mafia methods against the payment or the promise of money or other benefits.

In addition, the article 24-ter includes two types of criminal association characterized by their being set up to pursue specific crimes, namely: respectively, the offences relating to reducing into slavery, human trafficking and the smuggling of immigrants, organ trafficking, sexual crimes against minors and the offences of unlawful production, trafficking or possession of drugs of abuse or psychotropic substances. Some of these specific purpose-oriented offences are in themselves autonomous Predicate offences giving rise to the Entity's liability in the section on transnational crimes.

Specifically, Organized crimes offences, set out in Article 24-ter of the Decree, include:

- **Criminal association (Article 416 of the Criminal Code)**: punishes cases where three or more persons associate in order to commit several offences. It also makes punishable the leaders and those who promote, constitute, organise or participate in the association.
- **Mafia-type association including foreigners (Article 416-bis of the Criminal Code)**: anyone who is part of a mafia-type association consisting of three or more persons is liable for this offence. It also makes punishable the leaders and those who promote, constitute or organise the association.
- **Political-mafia electoral exchange (Article 416-ter of the Criminal Code)**: anyone who accepts the promise to procure votes with the use of the mafia method in exchange for the disbursement or promise of disbursement of money or other utilities and anyone who promises to procure votes with the use of that method is liable for this offence.
- **Kidnapping for the purpose of extortion (Article 630 of the Criminal Code)**: anyone who kidnaps a person for the purpose of obtaining, for himself or others, an unfair profit as the price of release is liable for this offence.
- **Association for the purpose of illegal trafficking in narcotic or psychotropic substances (Article 74 of Presidential Decree No. 309 of 9 October 1990)**: punishes the case in which three or more persons associate in order to cultivate, produce, manufacture, extract, refine, sell, offer or put up for sale, assign, distribute, trade, transport, procure for others, send, pass or send in transit, deliver for any purpose narcotic or psychotropic substances.
- **Illegal manufacture, introduction into the State, offering for sale, transfer, possession and carrying in a public place or place open to the public of weapons of war or war-like weapons or parts thereof, explosives, clandestine weapons as well as more common firing weapons, excluding those provided for in Article 2, paragraph 3, of Law No. 110 of 18 April 1975 (Article 407, paragraph 2, lett. a), number 5), Criminal Code)**:

anyone who, without a licence from the authorities, manufactures or introduces into the State or offers for sale or sells for any reason or illegally possesses or possesses war or warlike weapons, or parts thereof, suitable for use, war ammunition, explosives of any kind, chemical aggressors or other deadly devices, or collects them, shall be liable for this offence.

1.2. General rules of conduct

The cases of organised crimes offences can be potentially configured with reference to almost all the processes/activities identified at risk for 231 purposes, all the protocols identified for each of them will be applicable.

It should be noted that the Branch has adopted the Code of Conduct and the Code of Ethics, expressing the values and policies of the Branch, which set out the

- The following general principles of conduct addressed to all Recipients of the Model verify in advance the available information on business partners, suppliers, partners and consultants, in order to ascertain their respectability and the legitimacy of their activities before establishing these business relationships;
- operates in such a way as to avoid any implication in suitable operations, even potentially, to favor the realization of organized crime offences;
- verification of the actions of employees by the Departments in charge;
- prohibition of entering into banking relations or carrying out banking transactions with persons suspected of having relations with criminal organisations;
- prohibition to behave in such a way as to constitute the offences contemplated in this Section.

In general, the Branch's organisational system must comply with the basic requirements of formalisation and clarity, communication and separation of roles in compliance with the delegations and powers of attorney assigned.

1.3 Risky Activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

Organised crime offences, by their nature, extend the pervasiveness of the risk to all the Branch's operational areas and have therefore been considered to be a diffuse risk.

All Risky Activities as well as the relevant safeguards are to be generally recalled with regard to such offences. In particular, the activities in which the risk of organised crime offences is higher include:

1. Banking Supervisory Authorities relationship
2. Pubblic Administration relationship
3. Staff selection, recruitment and management
4. Management of gifts
5. Customer relationships

6. Customer account management and monitoring
7. Credit-related activities
8. Management of payments
9. Procurement of goods and services and appointment of professional assignments
10. Management of litigation and out-of-court procedures
11. Data and Information Systems Management
12. Accounting
13. Managing relations with Business Partners and Financial Intermediaries
14. Occupational Health and Safety Management
15. Tax management
16. Marketing and sales strategies
17. Waste production, discharges, air emissions and soil pollution

Since organised crime offences are considered an aggravating circumstance of the predicate offences provided for in the Decree, reference is made to the mitigation measures provided for the processes described in the related predicate offences.

FOURTH SECTION– CRIMES RELATING TO FORGERY OF MONEY AND VALUE AND CRIMES AGAINST INDUSTRY AND TRADE

1.1. Introduction

This Section includes the crimes provided for by Articles 25-bis and 25-bis.1 of the Decree, which concern the exercise of violence against property or the use of fraudulent means to prevent or disrupt the operation of an industry or commerce. For instance, this offence has been deemed to occur by those who enter in their website's source code – for the purpose of enhancing its visibility for search engines – keywords referable to a competitor's enterprise or products, in order to divert such competitor's potential customers.

The Article 25-bis of the Decree covers a series of offences listed in the Criminal Code, the aim being to protect public trust, which is society's reliance on the genuineness and integrity of certain specific symbols, which is essential to ensure the safe and timely performance of economic exchanges. The criminal conduct punished concerns coins, banknotes, cards and bearer's coupons issued by Governments or authorized Institutes – official stamps, watermark paper and instruments or objects intended for counterfeiting currency.

In addition, regarding the counteroffering this activity occurs where a mark is reproduced faithfully or its essential elements are imitated so as to appear authentic on initial perception. These are classified as material falsifications likely to harm public reliance on the fact that the products or services so marked come from the company which is the holder, licensee, or concessionaire of the registered mark. According to case law marks still unregistered are also protected, where an application has already been filed, since such application makes it formally knowable. For this

conduct to constitute an offence, it must be engaged in intentionally; intention may also exist where the author of the conduct, while not having the certainty that the mark has been registered (or that an application for registration has been filed), fails to implement the appropriate checks despite having reason to harbor such doubt.
In also punishes the conduct of counterfeiting, as well as the use, by another party who did not take part in the counterfeiting of patents, designs and industrial models belonging to others. This Article too aims at combating material counterfeiting which, in this type of offence, concerns documents proving the granting of the patents or model registrations.

Specifically, the crimes relating to forgery of money and value and crimes against industry and trade, set out in Articles 25-bis and 25-bis.1 of the Decree, include:

Art. 25-bis:

- **Counterfeiting of currency, spending and introduction into the State, with complicity, of counterfeit currency (Article 453 of the Criminal Code)**: anyone who counterfeits national or foreign currency, which is legal tender in the State or outside it, or alters genuine currency in any way, by giving it the appearance of a higher value, shall be liable for this offence; or anyone who, not being an accomplice in the counterfeiting or alteration, but in concert with the person who has carried it out or with an intermediary, introduces into the territory of the State or holds or spends or otherwise puts into circulation counterfeit or altered money or anyone who, in order to put them into circulation, purchases or in any case receives, from the person who forged them or from an intermediary, counterfeit or altered currency, or anyone who, legally authorised to produce it, unlawfully manufactures, by misusing the instruments or materials at his disposal, quantities of currency in excess of the prescriptions.
- **Alteration of currency (Article 454 of the Criminal Code)**: this offence is committed by anyone who alters currency, in any way diminishing its value, or manufactures counterfeit currency from scratch or anyone who, not being an accomplice to the counterfeiting or alteration, but in agreement with the person who has carried it out or with an intermediary, introduces into the territory of the State or holds or spends or otherwise puts counterfeit or altered currency into circulation or anyone who, in order to put it into circulation, purchases or in any case receives counterfeit or altered currency from the person who has counterfeited it or from an intermediary.
- **Spending and introduction into the State, without concert, of counterfeit currency (Article 455 of the Criminal Code)**: anyone who, outside the cases provided for in the two preceding Articles, introduces into the territory of the State, acquires or holds counterfeit or altered currency, in order to put it into circulation, or spends it or otherwise puts it into circulation, shall be liable for this offence.

- **Counterfeiting of revenue stamps, introduction into the State, purchase, possession or putting into circulation of counterfeit revenue stamps (Article 459 of the Criminal Code)**: this provision provides that Articles 453, 455 and 457 shall also apply to the counterfeiting or alteration of revenue stamps and to the introduction into the territory of the State, or to the purchase, possession or putting into circulation of counterfeit revenue stamps.
- **Counterfeiting of watermarked paper used for the manufacture of public credit cards or revenue stamps (Art. 460 of the Criminal Code)**: anyone who counterfeits watermarked paper used for the manufacture of public credit cards or revenue stamps, or purchases, holds or disposes of such counterfeit paper, shall be liable for this offence, unless the act constitutes a more serious offence.
- **Manufacture or possession of watermarks or instruments intended for the counterfeiting of currency, revenue stamps or watermarked paper (Article 461 of the Criminal Code)**: anyone who manufactures, acquires, possesses or alienates watermarks, computer programmes and data or instruments intended for the counterfeiting or alteration of currency, revenue stamps or watermarked paper shall be punished for this offence, unless the act constitutes a more serious offence. This offence shall also be committed if the aforementioned conduct relates to holograms or other components of the currency intended to ensure protection against counterfeiting or alteration.
- **Use of counterfeit or altered revenue stamps (Art. 464 of the Criminal Code)**: anyone who uses counterfeit or altered revenue stamps, without having taken part in the counterfeiting or alteration, shall be liable for this offence.
- **Counterfeiting, alteration or use of trademarks or distinctive signs or of patents, models and designs (Art. 473 of the Criminal Code)**: anyone who, being aware of the existence of an industrial property right, counterfeits or alters trademarks or distinctive signs, national or foreign, of industrial products, or anyone who, without being a party to the counterfeiting or alteration, makes use of such counterfeited or altered trademarks or signs, shall be liable for this offence, or anyone who counterfeits or alters national or foreign industrial patents, designs or models, or who, without having taken part in the counterfeiting or alteration, makes use of such counterfeited or altered patents, designs or models.
- **Introduction into the State and trade of products with false signs (Art. 474 of the Criminal Code)**: anyone who, except for cases of complicity in the offences provided for in Art. 473, introduces into the territory of the State, in order to make a profit, industrial products with counterfeit or altered trademarks or other distinctive signs, national or foreign, or anyone who,outside the cases of complicity in the offences provided for in Article 473, introduces into the territory of the State, holds for sale, offers for sale or otherwise puts into circulation, in order to gain profit, the products referred to above.

Art. 25-bis.1:

- **Obstructing freedom of industry or trade (Article 513 of the Criminal Code)**: this offence is committed by anyone who uses violence against property or fraudulent means to prevent or disrupt the exercise of an industry or trade, unless the act constitutes a more serious offence.
- **Unlawful competition with threats or violence (Article 513-bis of the Criminal Code)**: anyone who, in the exercise of a commercial, industrial or otherwise productive activity, engages in acts of competition with violence or threats is liable for this offence.
- **Fraud against national industries (Article 514 of the Criminal Code)**: anyone who causes damage to national industry by selling or otherwise putting into circulation, on national or foreign markets, industrial products with counterfeit or altered names, brands or distinctive signs, shall be liable for this offence.
- **Fraud in the exercise of trade (Article 515 of the Criminal Code)**: anyone who, in the exercise of a commercial activity, or in a shop open to the public, delivers to the purchaser a movable item for another, or a movable item, by origin, provenance, quality or quantity, different from that declared or agreed, shall be liable for this offence, unless the act constitutes a more serious offence.
- **Sale of non-genuine foodstuffs as genuine (Article 516 Criminal Code)**: anyone who offers for sale or otherwise markets as genuine non-genuine foodstuffs shall be liable for this offence.
- **Sale of industrial products with misleading signs (Article 517 of the Criminal Code)**: anyone who offers for sale or otherwise puts industrial works or products into circulation with names, trademarks or distinctive national or foreign signs, likely to mislead the buyer as to the origin, source or quality of the work or product, shall be liable for this offence, unless the act is provided for as an offence by another provision of law.
- **Manufacture of and trade in goods made by usurping industrial property rights (Article 517-ter of the Criminal Code)**: without prejudice to the application of Articles 473 and 474 of the Criminal Code, anyone who, being aware of the existence of an industrial property right, manufactures or industrially uses objects or other goods made by usurping an industrial property right or in breach thereof, or anyone who, in order to make a profit, introduces into the territory of the State, holds for sale, offers for sale directly to consumers or otherwise puts the above goods into circulation, shall be liable for this offence.
- **Counterfeiting of geographical indications or designations of origin of agri-food products (Article 517-quater of the Criminal Code)**: anyone who counterfeits or otherwise alters geographical indications or designations of origin of agri-food products or anyone who, for the purpose of making a profit, introduces into the territory of the State, holds for sale, offers for sale directly to consumers or otherwise puts the same products into circulation with counterfeit indications or designations shall be liable for this offence.

1.2. General rules of conduct

The following general principles of conduct addressed to all Recipients of the Model are designed to establish the rules of conduct in order to prevent the commission of offences provided in articles25-bis and 25-bis1 of Legislative Decree no. 231/01.

The Branch provides that all employees whose duties include the handling of valuables for whatever reason:

- must be specifically authorised in the specific operating procedures;
- have an obligation to operate with honesty, integrity, correctness and good faith;
- have an obligation to pay special attention to dealings with customers who are not sufficiently known to them, or to transactions concerning substantial amounts;
- must thoroughly check the valuables they receive, in order to identify any suspicious valuables.

1.3 Risky Activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Crimes relating to forgery of money and value and Crimes against industry and trade is generally higher concern the following:

1. Procurement of goods and services and appointment of professional assignments
2. Management of gifts
3. Customer relationships
4. Data and Information Systems Management
5. Marketing and sales strategies

1.3.1 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Obstructing freedom of industry or trade (Article 513 of the Criminal Code)
- Fraud against national industries (Article 514 of the Criminal Code)

By way of example, the offence could be committed in the event that the Branch engages in activities designed to disrupt and/or defraud industry, trade and competition by, for instance, entrusting a supplier with the task of counterfeiting or altering trademarks or distinctive signs, to the detriment of a competing bank and acts, for instance, to divert customers.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Policy on the Management of the External Legal Advisors
- Operating Expense Management Rules
- Financial Crime Policy
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Management of gifts

This Risk Activity mainly concerns processes related to:

a) Management of liberal initiatives;
b) Management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Obstructing freedom of industry or trade (Article 513 of the Criminal Code)
- Fraud against national industries (Article 514 of the Criminal Code)

By way of example, the offence could be committed in the event that the Branch, in the management of gifts, carries out activities likely to disrupt and/or defraud industry, trade and competition by circulating counterfeit or altered trademarks or distinctive signs.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Centralized Procurement Rules
- Conflict of interest Policy
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.3 Customer relationship

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Obstructing freedom of industry or trade (Article 513 of the Criminal Code)
- Fraud against national industries (Article 514 of the Criminal Code)

By way of example, the offences in question could occur if the Branch puts into circulation, on domestic or foreign markets, products with counterfeit or altered names, trademarks or distinctive signs likely to mislead customers.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Financial Crime Policy
- Credit Manual
- Banking Business Manual
- CIB Business Manual
- PEP Procedure
- Customer Due Diligence Archiving Procedure
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Complaint handling Procedure
- Anti-Internal Fraud Policy
- BRAINS Manual
- DAC-6 procedure
- CRS procedure
- FATCA Procedure
- Tax Affair Management Procedure
- Gifts and Entertainment Policy
- Measures Staff Recruitment
- Operating Expense Management Rules
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

- Staff Handbook

1.3.4 Data and Information Systems Management

This Risk Activity concerns processes related to:

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;
b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Obstructing freedom of industry or trade (Article 513 of the Criminal Code)
- Fraud against national industries (Article 514 of the Criminal Code)

By way of example, these offences could occur if the Branch uses altered software or databases, for instance, to conceal offences committed by the Branch or otherwise to its advantage.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Guidelines on System and Network Management
- ICBC (Europe) S.A. Breach Management Procedure
- ICBC (Europe) S.A. Data Retention Policy
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- ICBC (Europe) S.A. Milan Branch Employer Personal Data Policy
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Rules of IT General Management

- ICBC (Europe) S.A. Rules of Privacy by Design and Privacy by Default
- ICBC Privacy policy
- Information Security Policy
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- IT Governance-Equipment Management
- Measures of Information and Information System Security Management
- Milan Branch Employer Personal Data Processing Policy
- Power of attorney Branch to HQ data transfers GDPR
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- Security Management-Network&System Security
- Social Media Policy
- Technical Specifications for Security Technique for Network System
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.5 Marketing and sales strategies

This Risk Activity concerns processes related to:

a) promotion of the Branch's image on the Italian market;
b) development of marketing and sales strategies;
c) management of relations with prospects;
d) organisation of meetings with potential clients;
e) management of external reporting;
f) management of the proposition of new products, services or activities of the Branch (Definition of business needs; Preliminary investigation and evaluation of new products/services; Approval of new products/services).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Obstructing freedom of industry or trade (Article 513 of the Criminal Code)
- Unlawful competition with threats or violence (Article 513-bis of the Criminal Code)
- Fraud against national industries (Article 514 of the Criminal Code)
- Fraud in the exercise of trade (Article 515 of the Criminal Code)

- Counterfeiting, alteration or use of trademarks or distinctive signs or of patents, models and designs (Art. 473 of the Criminal Code)
- Introduction into the State and trade of products with false signs (Art. 474 of the Criminal Code)

By way of example, the offences in question could occur if the Branch places on the market banking products with characteristics other than those declared or agreed upon, with reference, for instance, to their origin, provenance or quality, by providing information likely to mislead the purchasers of the product, or if it places on the market products, by counterfeiting or altering trademarks or distinctive signs, whether domestic or foreign, in order to make a profit.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Procedure for Assessment and Approval of New Product
- ICBC Milan Branch Business Processing Procedures of Financial Markets Business
- ICBC EUROPE S.A. Milan Branch Administrative Measures for Financial Markets Business
- Financial Crime Policy
- Anti Internal Fraud Policy
- CIB Business Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Anti-Bribery and Corruption Policy
- Internal Operation and Management Authorization
- Financial Accounting Manual
- Responsibilities of Financial Accounting & IT Department
- Centralized Procurement Rules
- Treasury manual
- Banking Business Manual;
- Dac-6 procedure
- CRS procedure
- Procedure on the management of external legal advisors
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Tax Affair Management Procedure

- Gifts and Entertainment Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. accurate verification of the necessary qualifications, skills and requirements of suppliers;
2. adequately formalised requests for tenders addressed to suppliers;
3. traceability of access and critical activities carried out through the Branch's IT systems;
4. traceability of all IT events, problems and changes to the Branch's IT system;
5. archiving of documentation relating to the introduction of new products;
6. clear identification of the people/departments in charge of managing gifts, presents, sponsorships, entertainment expenses and charities
7. formal definition of the process for requesting, verifying and approving gifts, gratuities, sponsorships, entertainment expenses and charities
8. provision of specific value thresholds for the approval of gifts and gratuities;
9. periodic monitoring/control activities on the Branch's operations also by the Surveillance Body;
10. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
11. staff awareness activities in the areas of the Branch's operations.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 25-bis.1 of the Decree "Crimes against Industry and Trade", the following should be noted:

1. the New Product Assessment Committee supports the decision-making process of the Branch in the assessment and approval of new products;
2. the competent Branch Departments carry out feasibility assessments for the development of new products/services which are submitted to the New Product Evaluation Committee;
3. a thorough check is carried out on the compliance of the features and operation of the new products/services with the applicable regulations and internal rules, which is submitted to the New Products Evaluation Committee.

FIFTH SECTION - CORPORATE OFFENCES

1.1. Introduction

Article 25-ter of the Decree covers almost all corporate offences envisaged in Title XI of the Civil Code that qualify as general offences, in that they are not specifically referable to the exercise of banking activity.

The corporate offences considered concern various areas and relate in particular to the preparation of the financial statements, external communications, certain capital transactions, obstructing controls and hindering the performance of supervisory functions. All these types of offences have been defined for the common purpose of ensuring transparency of accounting documents and corporate management and the provision of sound information to shareholders, third parties and the market in general.

Specifically, Corporate offences, set out in Article 25-ter of the Decree, include:

- **False corporate reporting (Article 2621 of the Civil Code)**: this offence is committed by directors, general managers, managers responsible for preparing company accounting documents, statutory auditors and liquidators, except in the cases provided for in Article 2622 of the Civil Code, who, in order to obtain an unjust profit for themselves or others, knowingly state material facts in financial statements, reports or other corporate communications addressed to shareholders or the public, as required by law, which are not true, or omit material facts whose disclosure is required by law on the economic, asset or financial situation of the company or the group to which it belongs, in a manner which is likely to mislead others, even when the falsehoods or omissions concern assets owned or administered by the company on behalf of third parties.
- **Trivial offences (Article 2621-bis of the Civil Code)**: unless they constitute a more serious offence, a sentence of six months to three years' imprisonment shall be imposed if the facts referred to in Article 2621 of the Civil Code are of minor importance, taking into account the nature and size of the company and the manner or effects of the conduct. Unless they constitute a more serious offence, the same penalty as in the preceding paragraph shall apply where the facts referred to in Article 2621 concern companies that do not exceed the limits indicated in the second paragraph of Article 1 of Royal Decree No. 267 of 16 March 1942.
- **False corporate communications by listed companies (Article 2622 of the Civil Code)**: This offence is committed by directors, general managers, managers responsible for preparing company accounting documents, auditors and liquidators of companies issuing financial instruments admitted to trading on a regulated market in Italy or another European Union country, who, in order to obtain an unjust profit for themselves or others, in financial statements in financial statements, reports or other corporate communications addressed to

shareholders or the public, knowingly present untrue material facts or omit material facts whose disclosure is required by law on the economic, asset or financial situation of the company or of the group to which it belongs, in a manner likely to mislead others, even when the falsehoods or omissions concern assets owned or administered by the company on behalf of third parties.

The above-mentioned companies are equated with

- companies issuing financial instruments for which a request for admission to trading on an Italian or other European Union regulated market has been submitted;
- companies issuing financial instruments admitted to trading on an Italian multilateral trading facility
- companies controlling companies issuing financial instruments admitted to trading on an Italian regulated market or another European Union country; 4) companies calling on or otherwise managing public savings.

- **Obstruction of controls (Article 2625 paragraph 2 of the Civil Code)**: this offence is committed by directors who, by concealing documents or using other suitable devices, prevent or in any case obstruct the performance of control activities legally assigned to shareholders or other corporate bodies.
- **Unlawful repayment of contributions** (Article 2626 of the Civil Code): this offence is committed by directors who, except in cases of lawful reduction of share capital, return capital contributions to shareholders or release them from the obligation to make them, even if only simulated.
- **Unlawful distribution of profits and reserves (Article 2627 of the Civil Code)**: the directors liable for this offence are those who distribute profits or advances on profits that have not actually been earned or are allocated by law to reserves, or who distribute reserves, even if not established with profits, which may not be distributed by law, unless the act constitutes a more serious offence.
- **Unlawful dealing in the stocks or shares of the company or its parent company (Article 2628 of the Civil Code)**: this offence is committed by directors who, except in cases permitted by law, purchase or subscribe to shares or quotas of the company, thereby damaging the integrity of the share capital or of reserves that cannot be distributed by law, or purchase or subscribe to shares or quotas issued by the parent company, thereby damaging the share capital or reserves that cannot be distributed by law.
- **Transactions prejudicial to creditors (Article 2629 of the Civil Code)**: this offence is committed by directors who, in breach of the legal provisions protecting creditors, carry out share capital reductions or mergers with other companies or demergers, causing damage to creditors.
- **Failure to disclose conflict of interest (Article 2629-bis of the Civil Code)**: this offence

is committed by the director or member of the management board of a company with securities listed on regulated markets in Italy or in another Member State of the European Union or widely distributed among the public, who has, on his own behalf or on behalf of third parties, an interest in a given transaction that conflicts with that of the Company, fails to duly inform the other directors and refrains from taking part in resolutions concerning that transaction.

- **Fictitious capital formation (Article 2632 of the Civil Code)**: this offence is committed by directors and contributing shareholders who, even in part, fictitiously form or increase the share capital by allocating shares or quotas in excess of the total amount of the share capital, reciprocal subscription of shares or quotas, significant overvaluation of contributions in kind or receivables or of the assets of the company in the case of transformation.
- **Wrongful distribution of company assets by liquidators (Article 2633 of the Civil Code):** this offence is committed by liquidators who, by distributing company assets among the shareholders before paying the company's creditors or setting aside the sums necessary to satisfy them, cause damage to the creditors,
- **Bribery among private individuals (Article 2635 of the Civil Code)**: directors, general managers, managers responsible for drawing up the corporate accounting documents, auditors and liquidators, of private companies or bodies, or those who, within the organisational framework of the company or private body, perform management functions other than the persons mentioned above, are liable for this offence, who, unless the act constitutes a more serious offence, also through a third party, solicit or receive, for themselves or for others, undue money or other benefits, or accept the promise thereof, in order to perform or omit an act in breach of the obligations inherent in their office or of the obligations of loyalty or whoever, also through an intermediary, offers, promises or gives undue money or other benefits to the above-mentioned persons.
- **Instigating bribery among private individuals (Article 2635-bis of the Civil Code)**: this offence is committed by anyone who offers or promises money or other benefits not due to directors, general managers, managers responsible for preparing company accounting documents, statutory auditors and liquidators, of private companies or bodies, or to those who work in them and perform management functions, in order that they perform or omit an act in breach of the obligations inherent in their office or obligations of loyalty, if the offer or promise is not accepted, or to directors general managers, managers responsible for preparing the company's financial reports, auditors and liquidators, of companies or private entities, as well as those who perform management functions within them, who solicit for themselves or others, including through third parties, a promise or donation of money or other benefits, in order to perform or omit an act in breach of the obligations inherent in their office or obligations of loyalty, if the offer or promise is not accepted.

- **Unlawfully influencing the shareholders' meeting (Article 2636 of the Civil Code):** this offence is committed by anyone who, by simulated or fraudulent acts, determines the majority in the shareholders' meeting, in order to obtain an unjust profit for himself or others.
- **Market rigging (Article 2637 of the Civil Code)**: this offence is committed by anyone who disseminates false information, or who carries out simulated transactions or other artifices concretely likely to cause a significant alteration in the price of unlisted financial instruments or for which no application for admission to trading on a regulated market has been made, or to have a significant effect on the public's confidence in the financial stability of banks or bank groups.
- **Obstructing the activities of public regulatory authorities (Article 2638, Sections 1 and 2, of the Civil Code)**: this offence is committed by directors, general managers, managers responsible for preparing company accounting documents, statutory auditors and liquidators of companies or entities and other persons subject by law to public supervisory authorities, or bound by obligations towards them, who, in communications to the aforementioned authorities required by law, in order to hinder the exercise of supervisory functions set out untrue material facts, even if subject to assessment, on the economic, asset or financial situation of those subject to supervision or, for the same purpose, conceal by other fraudulent means, in whole or in part, facts that they should have disclosed, concerning the same situation, even where the information concerns assets owned or administered by the company on behalf of third parties. Also liable for this offence are directors, general managers, managers in charge of drawing up the corporate accounting documents, auditors and liquidators of companies or entities and other persons subject by law to public supervisory authorities or bound by obligations towards them, who, in any form whatsoever, including by omitting the communications due to the aforementioned authorities, knowingly obstruct their functions.
- **False or omitted statements for the issue of the preliminary certificate (Article 54 of Legislative Decree 19/2023)**: this offence is committed by any person who, in order to make it appear that the conditions for the issue of the preliminary certificate have been fulfilled, draws up wholly or partly false documents, alters true documents, makes false statements or omits relevant information.

1.2. General rules of conduct

The Risky Activities must be carried out in compliance with the laws in force, the rules set out in this Model and, also but not limited, to what is provided for in the Code of Conduct and Code of Ethics, expression of the values and policies of the Branch.

The actions, operations and transactions carried out on behalf of the Branch must be inspired by the principles of:

- correctness, completeness and transparency of information

- formal and substantial legitimacy
- clear and truthful accounting in compliance with current regulations and according to established procedures.

With regard to communications to the public, the information must be correct and it is mandatory to communicate the existence of any interest or conflict of interest regarding the matters to which the information relates.

To the extent of local competence in Headquarter training, for all employees of the Branch it is prohibited:

- to expose false material facts in the financial statements, in branch records, reports or in other corporate communications aimed at the third parties, or omit information on the economic, equity or financial situation of the Branch whose disclosure is required by law, in order to mislead recipients or causing financial damage to the third parties;
- to prevent or hinder the performance of control or auditing activities legally attributed to the supervisory authorities or auditing company through destroying records;
- in the communications provided for by law to the aforementioned authorities, to set out facts that are not true to the economic, patrimonial or financial situation of the supervised parties or to conceal with other fraudulent means, in whole or in part, facts that should have communicated concerning the same situation.

Employees of the Branch, without prejudice to their no tipping-off obligation, are required to cooperate fully with appropriately authorized internal or external investigations.

However, the employees before communicating any information or documentation to external auditors or the competent Authorities or otherwise cooperating with them, they must always ensure that it is valid do considering applicable laws and regulations.

Accounting is strictly based on the general principles of truth, accuracy, completeness, clarity and transparency of the recorded data.

Every accounting transaction must be traced and properly documented in compliance with form and substance of the legislation and the procedures in force, in order to allow at any time, the complete reconstruction.

The Branch provides that the records must maintained in sufficient detail as to reflect accurately the services and transactions undertaken by the Branch, in accordance with the legal and regulatory requirements.

The Branch is committed to accuracy in tax-related records, and to tax reporting compliance with the overall intent and letter of applicable laws.

The balance sheet of the Branch must always be prepared in accordance with related accounting principles and shall, in all material respects, reflect a true and fair view of the financial condition and results of the Branch. The evaluation criteria refer to civil law, standards generally accepted and the

instructions issued by the Supervisory Authority.
In addition, in order to ensure maximum fairness and transparency in the management of accounting operations, employees are required to comply with the principles of accounting and organizational separation.
In their behavior, employees and collaborators are obliged to refrain from any act, whether active or omissive, which directly or indirectly violates the mentioned principles or the internal procedures that relate to the formation of accounting documents and external representation.
Any omissions, errors, falsifications of accounting entries or records must be promptly reported to the Branch's control bodies of Headquarter.
Regarding the eventually conflicts of interest, all employees of the Branch should be aware of the appropriate policy regarding the identification, prevention and management of conflict of interest.

In general, all conflicts of interest, also potential, must be communicated to the Branch, including the conflicts of interests that may be arising from investments, corporate opportunities, business or personal dealing.

The Legal & Compliance Department must clearly notify to clients cases in which the measures taken by the branch to prevent or manage conflicts of interest are not sufficient to ensure, with reasonable certainty, the prevention of risks of damage to client interests.

1.3 Risky Activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Corporate offences is generally higher concern the following:

1. Reporting
2. Operational cost management
3. Staff selection, recruitment and management
4. Customer account management and monitoring
5. Managing relations with Business Partners and Financial Intermediaries
6. Marketing and sales strategies
7. Accounting
8. Management of litigation and out-of-court procedures
9. Banking Supervisory Authorities relationship
10. Public Administration relationship
11. Management of gifts
12. Customer relationships
13. Credit-related activities

14. Management of payments
15. Procurement of goods and services and appointment of professional assignments
16. Tax management

1.3.1 Reporting

This Risk Activity concerns processes related to:

a) management of periodic reporting to the Head Office and Headquarter;
b) conflict of Interest Management and Internal Reporting.

The Branch has in place arrangements through which to ensure any potential conflicts of interest are managed effectively, thereby preventing any material risk of damage to clients.
The Segregation of functions obligation shall be met by segregating duties as appropriate to avoid conflicts of interests wherever possible. These duties are set out via job descriptions, procedure manuals and organization charts. Ensuring these duties remain segregated is the responsibility of line managers.

The management of relevant information, for the purpose of identifying conflicts of interest, is carried out by all Departments of the Branch, whose manager (or the Deputy General Manager depending on the case), will inform, promptly, the Legal & Compliance Department, which provides support and advice during the process of identification and monitoring of conflicts of interest and must record all conflicts of interest of which it becomes aware.

In the event that an employee of the Corporate & Investment Banking Department (hereinafter referred to as the “CIB” Department) finds him/herself in a situation that could constitute a case of conflict of interest (as defined in the relevant Conflicts of Interest Policy), he/she must refrain from carrying out any activity of the CIB Department of the Branch that relates to the conflict situation and, in any event, comply with all the provisions set out in the relevant Conflicts of Interest Policy adopted by the Branch. Any potential conflict of interest must be disclosed in accordance with the provisions of the above Policy.

The types of crime that are abstractly applicable and the related methods of committing them are listed below by way of example only, but not limited to:

- False corporate reporting (Article 2621 of the Civil Code)
- Failure to disclose conflicts of interest (Article 2629-bis of the Civil Code)
- False reports or communications from the audit firm (Article 27 of Legislative Decree no.39/2010)
- Obstruction of the duties of the Public Supervisory Authorities (Article 2638 of the Civil Code)

- Transactions prejudicial to creditors (Article 2629 of the Civil Code)
- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, conflict of interest may occur if personal interests interfere (or seem to interfere) with the Branch, thus hindering the effective and impartial performance of one's activities, or if inappropriate personal benefits are pursued based on the position held within the Branch.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Banking Business Manual
- Compliance Policy
- Compliance Charter
- Financial Crime Policy
- DAC 6 Procedure
- AML & Compliance Committee Charter
- Client relationship Acceptance Committee Charter
- Conflict of interest Policy
- Gift and Entertainment Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Operational cost management

This Risk Activity mainly concerns processes related to the review and approval of daily operational costs.

The General Manager is ultimately responsible for the operating expense management, all daily expenses shall be reviewed and approved by the General Manager but the expenses above 15.000€ are approved by the Financial Affairs Committee of the Branch.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, the bribery among private individuals could take place in the event that the GM accepts money from an employee and in change of approving personal expenses as operational expenses.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the of the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Operating Expense Management Rules
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit t Manual
- Banking Business Manual
- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Financial Accounting Manual
- Gift and Entertainment Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.3 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;

j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The General Manager approves the new recruitment and signs the relative employment contract, but for senior resources of Second Level Functions (Legal & Compliance Department and Risk Management Department) is required also the approval of the Headquarter.
Moreover, the General Managers are responsible to draw up working schedule and approving or assigning overtime work employee recruitment.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, the crime of bribery among private individuals is committed if an employee offers money to the GM in order to obtain the approval of employment as temporary or fixed-term employee of relatives or persons connected to potential customers of the Branch.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- HR Management System Instructions March 2023
- Measures Staff Recruitment
- Employer Personal Data Processing Policy
- Rights and duties of the employees' disciplinary measures
- Code of Ethics
- Code of Conduct
- Staff Handbook
- Operating Expense Management Rules
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Third-party Management Procedure
- Performance Appraisal Guidelines
- Training Policy

- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Gift and Entertainment Policy
- Anti Internal Fraud Policy

1.3.4 Customer account management and monitoring

This Risk Activity concerns processes related to:

a) customer account profile management
b) account opening/closing;
c) management of dormant customers, dormant accounts and possible re-activation;
d) deviations from standard tariffs;
e) monitoring of accounts and customer information;
f) RMA exchange operation with the correspondent bank;
g) management of account or other product usage anomalies.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, the offence of bribery among private individuals could arise where a client offers money or other benefits to a Branch employee in order not to report activities/transactions carried out on accounts involving conflicts of interest.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Banking Business Manual
- Credit Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Financial Crime Policy
- Suspicious Transaction Reporting Procedure
- Anti Internal Fraud Policy
- BRAINS Manual

- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Charter of Credit Committee
- Whistleblowing Policy
- Conflict of interest Policy
- Gift and Entertainment Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.5 Managing relations with Business Partners and Financial Intermediaries

This Risk Activity concerns processes related to:

a) identification and selection of business partners (insurance companies/brokers/agents);
b) monitoring the situation of similar local banks;
c) preparation, organisation and execution of the marketing plan.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, this kind of offense takes place when the Senior persons in charge of drawing up the corporate documents, and the persons who exercise directives in the organizational area - even by an interposed person - solicit or receive, for themselves or for others, money or other benefits not due, or accept the promise, to perform or to omit acts in violation of the obligations inherent in their office or fidelity obligations in the context of relations with business partners or financial intermediaries.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Banking Business Manual
- Credit Manual
- Operating Expense Management Rules
- AML-CTF Due Diligence and Client Onboarding Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch

- Complaint handling procedure
- International Settlement and Trade Finance Operation Manual
- Anti Internal Fraud Policy
- Financial Crime Policy
- Conflict of interest Policy
- Whistleblowing Policy
- Gift and Entertainment Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.6 Marketing and sales strategies

This Risk Activity concerns processes related to:

a) promotion of the Branch's image on the Italian market;
b) development of marketing and sales strategies;
c) management of relations with prospects;
d) organisation of meetings with potential clients;
e) management of external reporting;
f) management of the proposition of new products, services or activities of the Branch (Definition of business needs; Preliminary investigation and evaluation of new products/services; Approval of new products/services).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, this kind of offense could be configured if the responsible of the Department to concluding a sponsorship and obtaining a benefit / interest in the Branch, agrees on a donation or promise of money or other benefits, for himself or for others, or omitted activities, in violation of the obligations inherent in their office.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Procedure for Assessment and Approval of New Product

- ICBC Milan Branch Business Processing Procedures of Financial Markets Business
- ICBC EUROPE S.A. Milan Branch Administrative Measures for Financial Markets Business
- Procedure on the management of external legal advisors
- Financial Crime Policy
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- CRS procedure
- Suspicious Transaction Reporting procedure
- Tax Affair Management Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Anti Internal Fraud Policy
- Centralized Procurement Rules
- Treasury manual
- Banking Business Manual;
- Dac-6 procedure
- Financial Accounting Manual
- Responsibilities of Financial Accounting & IT Department
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct

1.3.7 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;
c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;
f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Headquarter.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- False corporate reporting (Articles 2621 and 2621 bis of the Civil Code)

- Fictitious capital formation (Article 2632 of the Civil Code)
- Unlawful repayment of contributions (Article 2626 of the Civil Code)
- Unlawful distribution of profits and reserves (Article 2627 of the Civil Code)
- Unlawful dealing in the stocks or shares of the company or its parent company (Article 2628 of the Civil Code)
- Transactions prejudicial to creditors (Article 2629 of the Civil Code)
- Failure to disclose a conflict of interest (Article 2629 bis of the Civil Code)
- Obstruction of the duties of the Public Supervisory Authorities (Article 2638 of the Civil Code)

By way of example, the crime of false corporate reporting could potentially occur in the case of accounting communications required by law to the supervisory authorities where facts don't correspond to the truth, on the economic, asset or financial situation of the Branch.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Accounting Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Credit Manual
- Anti Internal Fraud Policy
- Third Party Management Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.8 Management of litigation and out-of-court procedures

This Risk Activity concerns processes related to:

a) complaints management;
b) management of active and passive judicial/out-of-court disputes (civil, criminal, administrative, labour law - debt collection) also with the external professional's assistance;
c) managing and monitoring settlement agreements.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, the offence of bribery among private individuals could occur if an employee of the Branch offers money, goods or other benefits in order to prevent the submission of complaints by customers.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Legal function working manual
- Complaint handling Procedure
- Policy on the Management of External Legal Advisor
- Third-party Management Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Conflict of interest Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.9 Banking Supervisory Authorities relationship

This Risk Activity concerns processes related to:

a) processing/transmission of occasional or periodic reports to the Supervisory Authorities;
b) requests/applications for licenses and/or authorisations;
c) feedback and compliance with applications/requests from the Supervisory Authorities;
d) management of relations with the Officials of the Supervisory Authorities during their inspection visits;
e) monitoring remediation actions and reporting/informing the Supervisory Authority

The types of crime that are abstractly applicable and the related methods of committing them are

listed below:

- Obstruction of controls (Article 2625 paragraph 2 of the Civil Code)
- Obstruction of the duties of the Public Supervisory Authorities (Article 2638 of the Civil Code)

By way of example, the crime of obstacle to the exercise of functions of the Public Supervisory Authorities could potentially occur in the case of the realization of exposure, within the notifications to the Public Supervisory Authorities, of material facts that do not correspond to the truth, even if subject to assessment, on the Branch's economic, asset or financial situation; or fraudulent concealment, total or partial, of material facts related to the economic, patrimonial or financial situation of the Branch, which must be communicated to the Public Supervisory Authorities; or obstacle to the functions of the Public Supervisory Authorities, even if they omit the communications due to the aforementioned Authorities.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Procedure for management of external inspections
- Suspicious transaction reporting procedure
- Operating Expense Management Rules
- AUI and SARA reporting procedure
- CRS procedure
- FATCA procedure
- AnaCredit Reporting Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.10 Public Administration relationship

This Risk Activity concerns processes related to:

a) management of relations with Chambers of Commerce;
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding

hygiene and safety and/or authorisations, permits, concessions;

d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;
e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office ;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police, Guardia di Finanza);
h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g. INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- False corporate reporting (Article 2621 of the Civil Code)
- Obstruction of controls (Article 2625 paragraph 2 of the Civil Code)

By way of example, the offence in question could occur in the event that the Branch uses artifice or deception to transmit data, information and documents on the company's economic, asset or financial situation to the competent authorities in order to avoid sanctions or other measures.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Training Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

- Staff Handbook

1.3.11 Management of gifts

This Risk Activity mainly concerns processes related to:

a) Management of liberal initiatives;
b) Management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635 of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis of the Civil Code)

By way of example, the offence could arise if the Branch grants gifts of significant economic value, as well as improper hospitality or entertainment expenses, to private entities in order to obtain an undue advantage or benefit.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Centralized Procurement Rules
- Conflict of interest Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.12 Customer relationship

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;

d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635 of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis of the Civil Code)

By way of example, the offences in question could occur if a Branch employee accepts a promise of money from a customer in order to perform an act in breach of the obligations inherent in his office, such as, for example, failing to report credit risks.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Credit Manual
- Banking Business Manual
- Financial Crime Policy
- Customer Due Diligence Archiving Procedure
- BRAINS Manual
- DAC-6 procedure
- CRS procedure
- FATCA Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Complaint handling Procedure
- Anti-Internal Fraud Policy
- CIB Business Manual
- PEP Procedure
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure

- Tax Affair Management Procedure
- Conflict of interest Policy
- Whistleblowing Policy
- Measures Staff Recruitment
- Operating Expense Management Rules
- Third-party Management Procedure
- Gifts and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.13 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;
c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635 of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis of the Civil Code)

By way of example, the offences in question could occur if a Branch employee accepts a promise of money from a customer in order to perform an act in breach of the obligations inherent in his office, such as granting a loan without meeting the necessary credit requirements.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Credit Manual
- Financial Accounting Manual
- Financial Crime Policy
- AML & Compliance Committee Charter

- AML-CTF Due Diligence and Client Onboarding Procedure
- Anti Internal Fraud Policy
- Banking Business Manual
- Charter of Credit Committee
- CIB Business Manual
- Complaint handling procedure
- CRS procedure
- Dac-6 procedure
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Market Abuse Policy
- Procedure for Assessment and Approval of New Product
- Suspicious Transaction Reporting procedure
- Gifts and Entertainment Policy
- Tax Affair Management Procedure
- Treasury manual
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Conflict of interest Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.14 Management of payments

This Risk Activity concerns processes related to the management of the payment of sales/goods/services actually rendered/received.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635 of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis of the Civil Code)

By way of example, this offence could occur if the branch pays its suppliers more than the agreed remuneration in order to obtain an undue advantage.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted

by the Branch:

- Financial Crime Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Anti-Internal Fraud Policy
- Banking Business Manual
- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee
- Gifts and Entertainment Policy
- Suspicious Transaction Reporting Procedure
- Third-party Management Procedure
- Conflict of interest Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.15 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635 of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis of the Civil Code)

By way of example, the offence could occur where the Branch offers or promises sums of money or other benefits undue to a supplier, so that the same, in breach of the obligations inherent in his office

or of loyalty, allows or facilitates the sale of goods and services at a price lower than the market price.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the internal regulation adopted by the Branch:

- Operating Expense Management Rules
- Centralized Procurement Rules
- Policy on the Management of the External Legal Advisors
- General Governance Policy of ICBC Milan Branch
- Third-party Management Procedure
- Financial Crime Policy
- Internal Operation and Management Authorization
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Conflict of interest Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.16 Tax management

This Risk Activity concerns processes related to:

a) drafting, approving and sending tax declarations or payment forms;
b) direct and indirect taxes payments;
c) management of active/passive invoicing;
d) storage of accounting records.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Bribery among private individuals (Article 2635 of the Civil Code)
- Instigating bribery among private individuals (art. 2635 bis of the Civil Code)

By way of example, the type of offence in question could occur where the person responsible for preparing/archivingthe corporate accounting documents receives, for himself or others, undue money or other benefits to perform or omit an act in breach of the obligations inherent in his office.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Tax Affairs Management Procedure
- Financial Accounting Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Dac-6 procedure
- CRS Procedure
- FATCA Procedure
- Suspicious Transaction Reporting procedure
- Treasury Manual
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Conflict of interest Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. formal identification of persons with roles and responsibilities in accounting issues;
2. filing of tax records in order to accurately reflect the services and transactions carried out by the Branch;
3. provision of procedures for reporting any omissions, tampering, falsifications or negligence in the accounts or in the supporting documentation on which the accounting records are based;
4. implementation of all measures of an organisational-accounting nature necessary to extract the data and information for the correct compilation of the reports and their timely submission to the Supervisory Authority, in accordance with the procedures and timescales established by the applicable legislation;
5. checks on the completeness, correctness and accuracy of the information transmitted to the Supervisory Authorities and the Public Administration;
6. accurate verification of the necessary qualifications, skills and requirements of suppliers;

7. adequately formalised offer requests addressed to suppliers;
8. transparent decision-making processes that can be reconstructed over time concerning the conditions stipulated with customers;
9. definition of the methods and criteria underlying any amendments and/or renewals of the conditions stipulated with customers;
10. definition of controls on potentially anomalous transactions, in terms of amount, type, subject or frequency;
11. verification of the accuracy and completeness of the documentation connected with the recording of accounting entries;
12. archiving and preservation of the documentation produced;
13. traceability of accesses and critical activities carried out through the Branch's IT systems;
14. prompt identification of system vulnerabilities;
15. archiving of documentation relating to contracts with suppliers;
16. periodic monitoring of supplier's performance;
17. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
18. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
19. staff awareness activities in the areas of operations of the Branch.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 25-ter "Corporate Offences ", the following should be noted:

1. the Financial Accounting & IT Department reports periodically on financial accounting management to Headquarter and Head Office;
2. internal financial accounting management policies and procedures are supervised and updated to ensure their effectiveness and regulatory compliance;
3. if a significant financial criticality arises (e.g. audits by internal or external supervisory functions or bodies that require adjustments to the financial statements), it must be reported promptly by e-mail and recorded in the appropriate system (OA System);
4. the Branch has an effective internal fraud risk management system.

SIXTH SECTION - CRIMES FOR THE PURPOSES OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER

1.1. Introduction

Under Article 25-quater of the Decree an entity shall be punishable where the crimes for the purpose of terrorism or subversion of the democratic order provided for by the Criminal Code, the special

laws and by the International Convention for the Suppression of the Financing of Terrorism, are committed in the interest of or for the benefit of the entity.

The article of the Decree sets out no fixed or mandatory list of crimes but refers to any criminal offence whose author specifically pursues aims of terrorism or subversion of the democratic order. Are considered as included and applicable in full all the international restrictive measures in force, being those limitations (and related sanctions) often strictly linked to counter terrorism measures.

In particular, conducts can considers having terrorist purposes if have been committed and can cause considerable damage to a Country or international organization and are committed in order to intimidate the population or force public authorities or an international organization to perform or restrain from performing any deed or destabilize or destroy fundamental political, constitutional, economic and social structures, as well as the other conducts defined as terrorist or committed for the purpose of terrorism by conventions or other international law provisions which are binding for Italy.

In addition, regarding the subversion of the democratic order, the case law considers that this expression is not limited to the concept of violent political action alone, but should rather refer to the Constitutional order, and therefore to any means of political struggle aimed at subverting the democratic and constitutional order or at departing from the fundamental principles governing them.

The type of crimes included in this Section concern crimes committed against the State's domestic and international personality, against citizens' political rights and against foreign countries, their heads and their representatives.

A specific attention should be focused also on financial offences, naturally, if such offences are instrumental to the pursuit of the aims of terrorism or subversion of the democratic order.

In order to avoid any gaps, the Article 24, paragraph 4, of the Decree refers to the 1999 New York Convention having the intent and final purpose to promote the cooperation for the suppression of the fund collecting and financing in any form to be used for and for financing terrorist activities in general or in sectors and concerning methods that entail a greater risk, which are the object of international treaties (by way of example air and maritime transport, diplomatic representations, nuclear, etc.); all the applicable international restrictive measures have to be considered included.

Save the foregoing, in addition to the aforesaid provisions, other relevant offences are set out in special laws covering a broad range of criminal activities (e.g., concerning weapons, drug trafficking, etcetera). All the international provisions issued and applicable on financial instruments and related to banking and/or financial activities (including those deposited in accounts in the name and/or interest of customers and/or pledged or constituting guarantee), that can be issued or being related to entities connected to individuals submitted to restrictive and operational measures are also included.

Specifically, the crimes for the purposes of terrorism or subversion of the democratic order, set out

in Articles 25-quarter of the Decree, include:

- **Subversive associations (Article 270 of the Criminal Code)**: anyone who in the territory of the State promotes, sets up, organises, directs or participates in associations aimed at violently subverting the economic or social order constituted in the State or violently suppressing the political and legal order of the State, or anyone who reconstitutes, even under a false name or simulated form, subversive associations whose dissolution has been ordered, shall be liable for this offence.
- **Associations for the purpose of terrorism, including international terrorism or for subversion of the democratic order (Article 270 bis of the Criminal Code)**: anyone who promotes, sets up, organises, directs, finances or participates in associations that propose the perpetration of acts of violence for the purpose of terrorism or the subversion of the democratic order is liable for this offence.
- **Assistance to associates (Article 270 ter of the Criminal Code):** anyone who, except in cases of aiding and abetting, gives refuge or provides food, hospitality, means of transport, communication tools to any of the persons participating in the associations indicated in Articles 270 and 270-bis shall be liable for this offence.
- **Enlistment for the purpose of terrorism, including international terrorism (Article 270-quater of the Criminal Code)**: anyone who, outside the cases referred to in Article 270-bis, enlists one or more persons for the purpose of committing acts of violence or sabotage of essential public services, for the purpose of terrorism, even if directed against a foreign State, an institution or an international organisation, shall be liable for this offence.
- **Organising travel for the purpose of terrorism (Article 270-quater.1)**: this offence is committed by anyone who, outside the cases referred to in Articles 270-bis and 270-quater, organises, finances or propagandises travel to foreign territory for the purpose of carrying out the conduct for the purpose of terrorism referred to in Article 270-sexies.
- **Training for the purposes of terrorism, including international terrorism (Article 270 quinquies of the Criminal Code)**: this offence is committed by any person who, outside the cases referred to in Article 270-bis, trains or in any case provides instructions on the preparation or use of explosive materials, firearms or other weapons, harmful or dangerous chemical or bacteriological substances, as well as any other technique or method for carrying out acts of violence or sabotage of essential public services, or receives training, for the purposes of terrorism, even if directed against a foreign State, institution or international body.
- **Financing terrorist activities (Article 270 quinquies.1 of the Criminal Code)**: this offence is committed by anyone who, outside the cases referred to in Articles 270-bis and 270-quater.1, collects, disburses or makes available goods or money, howsoever realised,

intended to be used in whole or in part for the perpetration of the conduct for the purposes of terrorism referred to in Article 270-sexies, regardless of the actual use of the funds for the commission of the aforementioned conduct, or anyone who deposits or keeps the aforementioned goods or money.

- **Conduct for the purpose of terrorism (Article 270-sexies of the Criminal Code)**: Conduct for the purpose of terrorism includes conduct which, by its nature or context, is likely to cause serious damage to a country or an international organisation and is carried out in order to intimidate the population or force public authorities or an international organisation to perform or refrain from performing any act or destabilise or destroy the fundamental political, constitutional, economic and social structures of a country or an international organisation, as well as other conduct defined as terrorist or committed for the purpose of terrorism by conventions or other rules of international law binding on Italy.
- **Attacks for the purposes of terrorism or subversion (Art. 280 Criminal Code)**: anyone who, for the purposes of terrorism or subversion of the democratic order, attacks the life or safety of a person is liable for this offence.
- **Act of terrorism with deadly or explosive devices (Art. 280 bis of the Criminal Code)**: this offence is committed by anyone who, for the purposes of terrorism, unless the act constitutes a more serious offence, commits any act aimed at damaging movable or immovable property belonging to others, through the use of explosive or otherwise deadly devices.
- **Acts of nuclear terrorism (Art. 280 ter of the Criminal Code)**: anyone who, for the purposes of terrorism referred to in Article 270-sexies, procures for himself or others radioactive matter or chemical or bacteriological materials or aggressives; creates a nuclear device or otherwise comes into possession of one; uses radioactive matter or chemical or bacteriological materials or aggressives or a nuclear device; uses or damages a nuclear facility in such a way as to release or with the concrete danger that it will release radioactive matter is liable for this offense.
- **Kidnapping for the purpose of terrorism or subversion of the democratic order (Article 289 bis of the Criminal Code)**: anyone who kidnaps a person for the purpose of terrorism or subversion of the democratic order is liable for this offense.
- **Kidnapping for the purpose of coercion (Art. 289-ter of the Criminal Code)**: anyone who kidnaps a person or holds him or her in his or her power by threatening to kill, injure or continue to hold him or her in order to compel a third party, whether a state, an international organization among several governments, a natural or legal person or a collectivity of natural persons, to perform any act or to refrain from doing so, making the release of the kidnapped person conditional on such action or omission, shall be liable for this offense.
- **Instigation to commit any of the crimes provided for in Chapters 1 and 2 (Art. 302 of**

the Criminal Code): anyone who instigates someone to commit any of the crimes, not culpable, provided for in Chapters 1 and 2 of Title I "Of crimes against the personality of the state" for which the law establishes life imprisonment or imprisonment if the instigation is not accepted, or if the instigation is accepted but the crime is not committed, shall be liable for this crime.

- **Political conspiracy by agreement (Article 304 of the Criminal Code)**: those who agree for the purpose of committing one of the crimes specified in Article 302 are liable for this offense, if the crime is not committed.
- **Political conspiracy by association (Art. 305 of the Criminal Code):** those who (three or more persons) promote, constitute or organize an association or associate for the purpose of committing for the purpose of committing one of the crimes indicated in Article 302 shall answer for this offense.
- **Armed gang: formation and participation (Article 306 of the Criminal Code)**: those who form, promote, constitute or organize, subject an armed gang in order to commit one of the crimes indicated in Article 302 are liable for this offense.
- **Assistance to participants in conspiracy or armed gang (Art. 307, Criminal Code)**: anyone who, outside the cases of aiding and abetting, gives shelter or provides food, hospitality, means of transportation, means of communication to any of the persons participating in the association or armed gang is liable for this offense.
- **Possession, hijacking and destruction of an aircraft (L. No. 342/1976, Art. 1)**: anyone who by violence or threat commits an act directed at the possession of an aircraft and anyone who by violence, threat or fraud commits an act directed at the hijacking or destruction of an aircraft is liable for this offense.
- **Damage to ground facilities (L. No. 342/1976, Art. 2)**: anyone who, in order to hijack or destroy an aircraft, damages ground facilities related to air navigation or alters the manner in which they are used is liable for this offense.
- **Penalties (L. No. 422/1989, Art. 3)**: anyone who: by violence or threat, takes possession of a ship or fixed installation; or exercises control over it; endangers the safety of navigation of a ship or the safety of a fixed installation; destroys or damages the ship or its cargo or installation; destroys or seriously damages maritime navigation equipment or services, or seriously alters their operation; intentionally communicates false information pertaining to navigation; commits acts of violence against a person on board the ship or installation.
- **New York Convention of December 9, 1999 (Art. 2):** any person who, including in the form of attempt, by any means, directly or indirectly, unlawfully and intentionally provides or collects funds with the intent to use them or knowing that they are intended to be used, in whole or in part, for the purpose of doing:

a) an act constituting an offense under and as defined in any of the treaties listed in the Annex; or
b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person who is not an active participant in situations of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or international organization to do or to refrain from doing something.

A crime is also committed by anyone who:

a) takes part as an accomplice in the commission of an offense referred to above;
b) organizes or directs other persons for the purpose of committing an offense referred to above;
c) contributes to the commission of one or more of the above crimes with a group of persons acting with a common purpose. Such contribution must be intentional and:
d) must be made for the purpose of facilitating the criminal activity or purpose of the group, where such activity or purpose involves the commission of an offense, referred to above;
e) must be made with the full knowledge that the intent of the group is to commit an offense referred to above.

1.2. General rules of conduct

In order to prevent the commission of the crimes provided for in Art. 25-quater of Legislative Decree 231/01, the Branch introduced the prohibition for all its employees to participate, organize, facilitate behaviors with purposes of terrorism or subversion of the democratic order.

In particular, it is forbidden to finance and collect money, directly or indirectly, for the purpose of using them or knowing that they will be used for the commission of crimes including those for purposes of terrorism or subversion of the democratic order.

The Branch carries out its activity in full compliance with the legislation against the crimes of terrorism and subversion of the democratic order, refusing to carry out suspicious and / or anomalous operations.

Accordingly, in the context of the implementation of legislative and regulatory requirements in the fight against money laundering and terrorist financing and other predicate offences (including corruption), the Branch does not enter into or maintain a relationship with any person or group (i) whose principal activity is engaged in activities classified as prohibited due to the risk of money laundering and terrorist financing; (ii) listed on any official sanctions list or whose beneficial owner or shareholder (50% or more) is a sanctioned person.

1.3. Risky activities pursuant to Legislative Decree no. 231/01 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Crimes for the purposes of Terrorism or Subversion of the Democratic Order is generally higher concern the following:

1. Customer relationships
2. Customer account management and monitoring
3. Credit-related activities
4. Staff selection, recruitment and management
5. Management of gifts
6. Procurement of goods and services and appointment of professional assignments
7. Management of payments
8. Accounting
9. Managing relations with Business Partners and Financial Intermediaries
10. Management of litigation and out-of-court procedures

1.3.1 Customer relationships

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)

- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime in question could take place in the case of funding and / or maintaining relationships with persons that are among the names included in the lists provided by the Authorities of Public Security, the Bank of Italy and the FIU because they are suspected of terrorism or subversion of the democratic order, or with other subjects suspected to be involved in these activities, as well as included in the lists of persons subject to international restrictive measures (including those concerning the embargo) or other operational restrictions, or including those subjects that carry out suspected activities at risk of money laundering too.
The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Suspicious Transaction Reporting Procedure
- Credit Manual;
- FATCA Procedure
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Banking Business Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Credit Manual
- CIB Business Manual
- Anti Internal Fraud Policy
- PEP Procedure
- Customer Due Diligence Archiving Procedure
- BRAINS Manual
- DAC-6 procedure
- CRS procedure
- Tax Affair Management Procedure
- Gifts and Entertainment Policy
- Measures Staff Recruitment
- Operating Expense Management Rules

- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Customer account management and monitoring

This Risk Activity concerns processes related to:

a) customer account profile management
b) account opening/closing;
c) management of dormant customers, dormant accounts and possible re-activation;
d) deviations from standard tariffs;
e) monitoring of accounts and customer information;
f) RMA exchange operation with the correspondent bank;
g) management of account or other product usage anomalies.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime in question could occur in the event that the Branch omits or improperly carries out the activities of performing the Adequate Verification with respect to the customer for the opening of the linked current account by proceeding to authorize the operations of persons included in the lists of the Public Security Authorities, by the Bank of Italy and the Financial Intelligence Unit because they are suspected of conduct with terrorist aims or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy

- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Internal Operation and Management Authorization
- Banking business manual
- BRAINS Manual
- Anti Internal Fraud Policy
- Charter of Credit Committee
- Conflict of interest Policy
- Credit Manual
- General Governance Policy of ICBC Milan Branch
- Gifts and Entertainment Policy
- Whistleblowing Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.3 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;
c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime in question could occur in the event that the Branch produces altered documents in order to grant financing without the necessary credit requirements being met to persons included on the lists of the Public Security Authorities, by the Bank of Italy and the Financial Intelligence Unit because they are suspected of conduct with terrorist aims or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Suspicious Transaction Reporting procedure
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Banking Business Manual
- Internal Operation and Management Authorization
- Anti Internal Fraud Policy
- Charter of Credit Committee
- CIB Business Manual
- Complaint handling procedure
- Credit Manual
- CRS procedure
- Dac-6 procedure
- Financial Accounting Manual
- General Governance Policy of ICBC Milan Branch
- Gifts and Entertainment Policy
- Market Abuse Policy
- Procedure for Assessment and Approval of New Product
- Tax Affair Management Procedure
- Treasury manual
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.4 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime could occur in the event that the Branch in order to obtain undue advantages or utilities, could hire persons included in the lists of the Public Security Authorities, by the Bank of Italy and the Financial Intelligence Unit because they are suspected of holding conduct with terrorist aims or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- General Governance Policy of ICBC Milan Branch

- Internal Operation and Management Authorization
- Employer Personal Data Processing Policy
- Rights and duties of the employees' disciplinary measures
- HR Management System Instructions March 2023
- Measures Staff Recruitment
- Operating Expense Management Rules
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Third-party Management Procedure
- Performance Appraisal Guidelines
- Training Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.5 Management of gifts

This Risk Activity mainly concerns processes related to:

a) Management of liberal initiatives;
b) Management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime could occur in the event that the Branch in order to obtain undue advantages or utilities, could give gifts of significant economic value, as well as make improper hospitality or entertainment expenses to persons linked, directly or indirectly, to associations with

the purpose of terrorism or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Centralized Procurement Rules
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.6 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion

of the democratic order (Article 270-bis of the Criminal Code)

- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime could occur if the Branch, in order to obtain undue advantages or utilities, confers professional assignments to persons included in the lists of the Public Security Authorities, by the Bank of Italy and the Financial Intelligence Unit because they are suspected of holding conduct with terrorist aims or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Centralized Procurement Rules
- Policy on the Management of the External Legal Advisors
- Operating Expense Management Rules
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.7 Management of payments

This Risk Activity concerns processes related to the management of the payment of sales/goods/services actually rendered/received.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-

bis of the Criminal Code)

- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the crime could occur if the Branch carries out improper management of purchases with the intention, or mere awareness, that the money or goods connected with the relevant transactions will be intended to be used, in whole or in part, for the purpose of financing terrorism.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Financial Affairs and Centralized Procurement Management Committee
- Suspicious Transaction Reporting Procedure
- Internal Operation and Management Authorization
- Operating Expense Management Rules
- Anti-Internal Fraud Policy
- Banking Business Manual
- Centralized Procurement Rules
- General Governance Policy of ICBC Milan Branch
- Gifts and Entertainment Policy
- Third-party Management Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.8 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;
c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;

f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Head Quarter

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, the type of crime in question could occur in the event that the Branch in order to obtain undue advantages or benefits, in financial statements, reports or other corporate communications, knowingly omits, in whole or in part, material facts that are relevant, or exposes material facts that are untrue having as their object, for example, varying existing accounts, or overstating receivables, or accounting for costs for goods and services not received or recording nonexistent transactions, in order to create extra-accounting funds to be allocated to persons linked, directly or indirectly, to associations with the purpose of terrorism or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Accounting Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Operating Expense Management Rules
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Third Party Management
- Whistleblowing Policy

- Conflict of interest Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.9 Managing relations with Business Partners and Financial Intermediaries

This Risk Activity concerns processes related to:

a) identification and selection of business partners;
b) monitoring the situation of similar local banks;
c) preparation, organisation and execution of the marketing plan.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, this type of crime could occur if the Branch enters into contractual commitments with business partners that are directly or indirectly linked to associations that propose to carry out acts of violence for the purpose of terrorism or subversion of the democratic order.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Banking Business Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure
- Operating Expense Management Rules
- Complaint handling procedure

- Conflict of interest Policy
- International Settlement and Trade Finance Operation Manual
- Gifts and Entertainment Policy
- Anti Internal Fraud Policy
- Credit Manual
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.10 Management of litigation and out-of-court procedures

This Risk Activity concerns processes related to:

a) complaints management;
b) management of active and passive judicial/out-of-court disputes (civil, criminal, administrative, labour law - debt collection) also with the external professional's assistance;
c) managing and monitoring settlement agreements.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Financing terrorist activities (Article 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies (Article 270-quinquies 2 code of civil procedure)
- Kidnapping for purposes of terrorism or for subversion of the democratic order (Article 289-bis of the Criminal Code)
- Associations for the purpose of terrorism, including international terrorism, or of subversion of the democratic order (Article 270-bis of the Criminal Code)
- Crimes for the purpose of terrorism (1999 New York Convention)

By way of example, this offense could occur if the Branch, involved in litigation, destroys or alters documents revealing its involvement in activities related to the financing of terrorism.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Legal function working manual
- Policy on the Management of External Legal Advisor
- Internal Operation and Management Authorization

- General Governance Policy of ICBC Milan Branch
- Complaint handling procedure
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Third-party Management Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of the persons in charge of managing customer relationships;
2. transparent and reconstructible decision-making processes over time related to the conditions stipulated with customers;
3. identification of customers for anti-money laundering and counter-terrorist financing purposes;
4. clear identification of the people/departments in charge of managing and monitoring customers' accounts;
5. traceability in paper and/or electronic form of the conditions stipulated with customers;
6. verification of completeness and correctness of the documentation collected and/or prepared related to customer relationships;
7. periodic updating of information relating to customer relationships in order to enable constant assessment of the economic and financial profile as well as the risk of money laundering and terrorist financing;
8. definition of controls on potentially anomalous transactions, in terms of amount, type, object or frequency;
9. clear identification of the people/departments in charge of managing credit-related activities;
10. clear identification of the people/departments in charge of the purchase of goods and services and the awarding of professional appointments;
11. thorough verification of the necessary qualifications, skills and requirements of suppliers;
12. properly formalized requests for proposals addressed to suppliers;
13. periodic monitoring of suppliers' performance;
14. archiving of documentation relating to contracts with suppliers;
15. transparency of the process of recruitment and employment of personnel, motivated by actual business needs, based on non-arbitrary criteria and as objective as possible;

16. clear identification of the people in charge of managing the accounts;
17. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
18. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
19. staff awareness activities in the areas of operations of the Branch.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 25-quater "Crimes for the purposes of Terrorism or Subversion of the Democratic Order", the following should be noted:

1. the Corporate & Investment Banking Department shall identify and verify the identity of customers before opening an account and perform Customer Due Diligence (CDD) in accordance with the anti-money laundering and anti-terrorism regulations in force:
2. any abnormal behavior suspicious of terrorism must first be reported to the head of the relevant Department and, if applicable, immediately to the Money Laundering Reporting Officer (MLRO). The Legal and Compliance Department or the MLRO, in case of escalation, will make the necessary investigation and possible reporting to the local Financial Intelligence Unit (FIU);
3. the Branch provides employees with access to up-to-date information on the practices of terrorist financiers, clues leading to the recognition of suspicious transactions, and organizes annual training;
4. the Branch adopts and maintains the Single Computer Archive (AUI) and periodically reports aggregate transaction data (S.A.R.A. reporting) to the FIU;

SEVENTH SECTION - CRIMES AGAINST INDIVIDUALS

1.1. Introduction

Article 25-quinquies of the Decree lists certain offences against individuals set out in the Criminal Code in order to forcefully combat new forms of slavery such as prostitution, human trafficking, the exploitation of children and forced begging.

As for the crimes included in this Section, some are considered significant in the event that a Branch representative or employee acts in conspiracy with the material author of the offence. The type of conspiracy where risk is greatest is linked to financing by the Branch of organizations or of persons that commit any of the above-mentioned offences. In particular with references to crime related to slavery, prostitution, or activities related to human trafficking.

In addition, are included in this Section and it must be taken into consideration as it is of particular relevance also the Illegal intermediation and exploitation of labor.

This crime concerns those who take advantage of the workers' needy status and intermediate, use,

hire or employ labour under conditions akin to exploitation.
Situations such as the payment of remuneration that does not align with the labor union contracts, repeated violation of the working hours and rest regulations, violation of the occupational health and safety regulations are included among the exploitation indices.
Specifically, Crimes against individuals, set out in Article 25-quinquies of the Decree, include:

- **Reduction or maintenance in slavery or servitude (Art. 600 of the Criminal Code):** anyone who exercises powers over a person corresponding to those of the right of ownership or anyone who reduces or maintains a person in a state of continuous subjection, forcing him or her to work or sexual services or to begging or otherwise to engage in illegal activities involving exploitation or to submit to the removal of organs is liable for this offense. The reduction or maintenance in the state of subjection takes place when the conduct is carried out through violence, threat, deception, abuse of authority or taking advantage of a situation of vulnerability, physical or mental inferiority or a situation of need, or through the promise or giving of sums of money or other benefits to those in authority over the person.
- **Child prostitution (Art. 600-bis of the Criminal Code)**: anyone who recruits or induces to prostitution a person under the age of eighteen years is liable for this offense: promotes, exploits, manages, organizes or controls the prostitution of a person under the age of eighteen years, or otherwise profits from it, or anyone who, unless the act constitutes a more serious offense, engages in sexual acts with a minor between the ages of fourteen and eighteen years, in exchange for consideration in money or other benefit, even if only promised.
- **Child pornography (Art. 600-ter of the Criminal Code):** anyone who, using minors under eighteen years of age, puts on pornographic performances or shows or produces pornographic material; recruits or induces minors under eighteen years of age to participate in pornographic performances or shows or otherwise profits from the aforementioned shows shall be liable for this offense. Whoever trades in the pornographic material referred to above; whoever by any means, including by telematic means, distributes, divulges, disseminates or publicizes the pornographic material referred to above, or distributes or divulges news or information aimed at the enticement or sexual exploitation of minors under eighteen years of age; whoever offers or transfers the pornographic material to others, including free of charge, or whoever attends pornographic performances or shows in which minors under eighteen years of age are involved.

  For the purposes of this article, child pornography is defined as any depiction, by whatever means, of a child under the age of eighteen involved in sexually explicit activities, real or simulated, or any depiction of the sexual organs of a child under the age of eighteen for sexual purposes.

- **Possession of or access to pornographic material (Art. 600-quarter of the Criminal Code)**: anyone who, outside the cases provided for in Article 600-ter, knowingly procures or possesses pornographic material made using minors under the age of eighteen years or anyone who, through the use of the Internet or other networks or means of communication, intentionally and without justified reason accesses pornographic material made using minors under the age of eighteen years is liable for this offense.
- **Virtual pornography (Art. 600-quater.1 of the Criminal Code)**: this provision provides that the provisions of Articles 600-ter and 600-quater also apply when the pornographic material represents virtual images made using images of minors under eighteen years of age or parts thereof. Virtual images are defined as images made using graphic processing techniques not associated in whole or in part with real situations, whose quality of representation makes non-real situations appear as real.
- **Tourist initiatives aimed at the exploitation of child prostitution (Art. 600-quinquies of the Criminal Code):** anyone who organizes or propagates trips aimed at the enjoyment of prostitution activities to the detriment of minors or otherwise including such activity is liable for this offense.
- **Trafficking in persons (Art. 601 of the Criminal Code):** anyone who recruits, introduces into the territory of the State, also transfers outside it, transports, transfers authority over the person, harbors one or more persons who are in the conditions referred to in Article 600, or, carries out the same conduct on one or more persons, by means of deception, violence, threat, abuse of authority or taking advantage of a situation of vulnerability, physical or mental inferiority or necessity, shall be liable for this crime, or by promising or giving money or other benefits to the person having authority over them, in order to induce or compel them to perform work, sexual services or begging or otherwise to engage in illegal activities involving their exploitation or to submit to the removal of organs, or anyone who, even outside the above-mentioned modalities, carries out the conducts provided for therein with respect to a person under the age of majority.
- **Purchase and alienation of slaves (Art. 602 of the Criminal Code):** anyone who, outside the cases indicated in Article 601, purchases or alienates or disposes of a person who is in one of the conditions referred to in Article 600 shall be liable for this offense.
- **Illicit intermediation and work exploitation (Article 603-bis of the Criminal Code):** anyone who, unless the fact constitutes a more serious crime, recruits labor for the purpose of assigning it to work for third parties under exploitative conditions, taking advantage of the workers' state of need; uses, hires or employs labor, including through the activity of intermediation, subjecting workers to exploitative conditions and taking advantage of their state of need, shall be liable for this crime.

For the purposes of this article, the existence of one or more of the following conditions constitutes an indication of exploitation:

1) the repeated payment of wages in a manner manifestly inconsistent with the national or territorial collective bargaining agreements entered into by the most representative trade unions at the national level, or otherwise disproportionate to the quantity and quality of work performed;
2) the repeated violation of regulations on working hours, rest periods, weekly rest, compulsory leave, vacations;
3) the existence of violations of regulations on safety and hygiene in the workplace;
4) the subjecting of the worker to degrading working conditions, surveillance methods or housing situations.

- **Child enticement (Art. 609-undecies of the Criminal Code):** anyone who, for the purpose of committing the crimes referred to in Articles 600, 600-bis, 600-ter and 600-quater, including those relating to pornographic material referred to in Articles 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies and 609-octies, entices a minor under the age of sixteen years, if the act does not constitute a more serious crime, shall be liable for this offense. Solicitation is defined as any act aimed at gaining the trust of a minor through artifice, flattery or threats carried out including through the use of the Internet or other networks or means of communication.

1.2. General rules of conduct

All employees are required to carefully observe the rules of conduct and must respect the fundamental principles of honesty, integrity in the performance of their activities.

The Branch believes that respect for the personality and dignity of each employee is fundamental in developing a work environment based on reciprocal trust and loyalty and which is enriched by the contribution of each individual.

The staff recruitment of the Branch is based refers to the process of selecting qualified persons from the outside of the Branch to work at suitable posts according to human resources planning and on certain principles and follow procedures in order to meet current and future development demands.

The staff recruitment follows the principle of “overall planning, demand-oriented, suitable matching, open and fair, in accordance with the law and regulations”, and shall adapt to operational transformation and business development, comply with personnel planning and personnel structure adjustment.

In the organization of the Branch are supports rights and opportunities for staff that must to be treated with dignity and respect while at work. All employees of the Branch are prohibited from facilitating or participating in the purposes of crimes against personal freedom.

The Branch shall approve the potential employees through human resource management system within the annual scope of authority. If the employment of a candidate is beyond the branch’s

approval authority, it shall be reported to the Headquarter for approval before the hired. The annual scope of authority shall be determined by Headquarter according to practical situation of all branches.

It is also ensured for all employees of the Branch an adequate working time and an adequate remuneration proportionated to the working hours.

1.3 Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Crimes against individual is generally higher concern the following:

1. Staff selection, recruitment and management
2. Procurement of goods and services and appointment of professional assignments

1.3.1 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Illicit intermediation and work exploitation (Art. 603-bis of the Criminal Code)

By way of example, the offense could take place in the case in which workers are imposed work schedules that are clearly contrary to the provisions of collective agreements and with disproportionate remuneration, or the workplace does not comply with the rules on safety or hygiene.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Measures Staff Recruitment
- Rights and duties of the employees' disciplinary measures
- Code of Ethics
- Code of Conduct
- Staff Handbook
- Employer Personal Data Processing Policy
- Performance Appraisal Guidelines
- Training Policy
- HR Management System Instructions March 2023
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of Interests Policy
- Anti Internal Fraud Policy
- Operating Expense Management Rules
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Third-party Management Procedure

1.3.2 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Illicit intermediation and work exploitation (Art. 603-bis of the Criminal Code)

By way of example, the offense could occur if professionals/consultants/suppliers are reiteratedly paid remuneration that is disproportionate to the quantity and quality of work performed.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Centralized Procurement Rules
- Operating Expense Management Rules
- Third-party Management Procedure
- Policy on the Management of the External Legal Advisors
- Internal Operation and Management Authorization
- Financial Crime Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of the persons/functions in charge of personnel selection, recruitment and administration and the assignment of professional positions;
2. transparency of the process of recruitment and employment of personnel, motivated by actual business needs, based on non-arbitrary criteria and as objective as possible;
3. definition of criteria related to the preparation of the economic offer;
4. traceability, storage and preservation of all documentation related to the process of selection and recruitment and personnel management;
5. clear identification of the people/departments in charge of the purchase of goods and services and the awarding of professional appointments with definition of specific spending powers;

6. thorough verification of necessary qualifications, skills and requirements of suppliers;
7. properly formalized requests for proposals addressed to suppliers;
8. periodic monitoring of suppliers' performance;
9. archiving of documentation related to contracts with suppliers;
10. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
11. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
12. staff awareness activities in the areas of the Branch's operations.

EIGHTH SECTION - MARKET ABUSE

1.1. Introduction

The Article 25-sexies of the Legislative Decree no.231/01 provides for the entity's administrative liability in cases of offences of "insider trading" and of "market manipulation", as laid down in Articles 184 and 185 of Legislative Decree no. 58/199 (Consolidated Law on Financial Intermediation, hereinafter the "Consolidated Law on Finance"),

On the other hand, in the administrative breaches referred to in Articles 187-bis and 187-ter, the Entity's liability arises from the provisions of Article 187-quinquies of the Consolidated Law on Finance, which refers to the same principles, conditions and exemptions set out in Legislative Decree no. 231/2001, yet places on the Entity the burden of proving that the perpetrator of the offence acted solely in his own or a third party's interest.

The above-mentioned rules are aimed at ensuring the integrity, transparency, correctness and efficiency of the financial markets, in accordance with the principle that all investors should operate on a level playing field with regard to access to information, knowledge of the pricing mechanism and knowledge of the source of publicly available information.

It should be noticed that under Article 182 of the Consolidated Law on Finance, the offences punishable according to Italian law even if committed abroad, where these offences involve financial instruments admitted to trading, or for which admission to trading has been requested, on an Italian regulated market or on a regulated market of other European Union Member States, or financial instruments admitted to trading on an Italian multilateral trading facility, for which admission has been requested or authorized by the issuer. Where the offence was committed in Italy, the same conduct is sanctioned if it concerns financial instruments admitted to trading on an Italian regulated market or on a regulated market of another European Union Member State, or for which such admission to trading has been requested, or where it concerns financial instruments admitted to trading on an Italian multilateral trading facility.

The highest risks of offences being committed can occur in the following scenarios: simulated transactions, other devices or insider trading of the Branch own property portfolio or through personal

dealing and dissemination of false or misleading news, especially concerning transactions carried out in the market before or after such dissemination.
Where the transactions requested by the customers give rise to suspicions that one of the offences of “Insider trading” or “market manipulation” might occur, under Article 187-nonies of the Consolidated Law on Finance the reporting obligation rests with the intermediary.

Specifically, Market Abuse offences, set out in Article 25-sexies of the Decree, include:

- **Market Manipulation (Art. 185 Legislative Decree No. 58/1998):** anyone who spreads false news or carries out simulated transactions or other artifices concretely capable of causing a significant alteration in the price of financial instruments is liable for this offense.
- **Abuse or unlawful communication of inside information**. **Recommending or inducing others to commit insider trading (Art. 184 Legislative Decree no. 58/1998)**: anyone who, being in possession of inside information by reason of his or her membership in the issuer's administrative, management or supervisory bodies, participation in the issuer's capital, or the exercise of a job, profession or function, including a public one, or office, shall be liable for this offense: a) buys, sells or performs other transactions, directly or indirectly, on his or her own behalf or on behalf of third parties, on financial instruments using such information;
    - discloses such information to others outside the normal course of employment, profession, function, or office, or a market survey carried out pursuant to Article 11 of Regulation (EU) No. 596/2014 of the European Parliament and of the Council of April 16, 2014;
    - recommends or induces others, on the basis of such information, to carry out any of the transactions referred to in subparagraph (a).
- **Prohibition of market manipulation (Art. 15 EU Reg. No. 596/2014):** this provision provides that it is not permitted to engage in market manipulation or attempt to engage in market manipulation.
- **Prohibition of insider trading and unlawful disclosure of inside information (Art. 14 EU Reg. No. 596/2014):** this provision provides that it is not permitted to:
    a) abuse or attempt to abuse insider information;
    b) recommend to others to abuse insider information or induce others to abuse insider information; or
    c) unlawfully communicate insider information.

1.2. General rules of conduct

According to the policy of the Branch, restricted information includes both inside information (that being information of a precise nature that, if made public, would significantly impact the price of

related securities) and confidential information, including material which may not necessarily be price sensitive and which may not obviously appear to be commercially sensitive.
The Branch's policy has to apply the principle that 'restricted information' can only be disclosed to any person where a legitimate 'need to know' is first established. This involves the establishment and maintenance of clear segregation of activities and tasks which act as information barriers controlling the disclosure of information and preventing its unauthorized release to other areas of the Branch.
The Branch's main segregation divides its businesses into two categories: the public side - employees who deal with customers and other departments described as private side because they routinely receive or have access to 'restricted information'

Restricted information for a particular transaction should be shared between a small group of only those who really need the information to carry out their duties This is typically the immediate 'deal team' and the control functions such as Legal & Compliance Department, IT Function, Risk Management. 'Restricted information' may only be passed between business areas in accordance with the 'need to know' principle and the segregation of duties.
The Branch prohibits its employees from dealing in the securities of any company when they are in possession of material, non-public information concerning the company. It is further prohibited to:

a. procuring or advising any other person to enter into such a transaction, and/or
b. communicating information or any opinion to another person if you know or should know that the person in question will carry out such a transaction.

If there is any doubt about the authorisation to proceed with trading in financial instruments, staff must consult with the Legal & Compliance Department before trading.

In addition, the branch pays particular attention also regarding the future information, speculative or contingent events, even if it is significant only when considered in combination with public available information.
Information is “non-public” unless it has been publicly disclosed, and adequate time has passed for the securities markets to digest the information. Example of adequate disclosure include public filings with securities regulatory authorities and the issuance of press releases and may also include meeting with members of the press and public.
The branch provides that is also prohibited pass on inside information to any other person if the employee knows or reasonably suspect that the person receiving such information from you will misuse such information by trading in securities or passing such information.

Any suspicious transaction and orders should immediately be notified to the competent authority thought a suspicious transaction and order report (“STOR”).
It is not acceptable to wait for enough suspicious orders or transactions to accumulate reporting.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Market Abuse Crimes is generally higher concern the following:

1. Own portfolio management
2. Reporting
3. Managing relations with Business Partners and Financial Intermediaries
4. Credit-related activities

1.3.1 Own portfolio management

This Risk Activity concerns processes related to:

a) identification, classification and management of inside information;
b) activities related to the possible use of inside information;
c) trading on financial instruments.

Restricted information for a particular transaction should be shared between a small group of only those who really need the information to carry out their duties This is typically the immediate 'deal team' and the control functions such as Legal & Compliance Department and Risk Management.
Restricted information for a particular transaction should be shared between a small group of only those who really need the information to carry out their duties This is typically the immediate 'deal team' and the control functions such as Legal & Compliance Department, Internal Audit, Risk Management.
The Legal & Compliance Department shall be in charge to manage the Policy based on the local Senior Management and Chief Compliance Officer (Luxembourg)’s requirements.
Management information relevant to identifying conflicts of interest is collected by any department of the Branch and communicated to the Legal & Compliance Department.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Insider trading (Article 184 of the Consolidated Law on Finance)
- Market manipulation (Article 185 of the Consolidated Law on Finance)

By way of example, this offence also occurs when such person discloses restricted information to others outside the normal exercise of his employment, profession, duties or position or when he recommends or induces others, on the basis of such information, to carry out trading operations of financial instruments.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Market Abuse Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Charter of Credit Committee
- Conflict of interest Policy
- Whistleblowing Policy
- International Settlement and Trade Finance Operation Manual
- CIB Business Manual
- AML-CTF Due Diligence and Client Onboarding Procedure
- ICBC Milan Branch Business Processing Procedures of Financial Markets Business
- ICBC EUROPE S.A. Milan Branch Administrative Measures for Financial Markets Business
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Reporting

This Risk Activity concerns processes related to:

a) management of periodic reporting to the Head Office;
b) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Insider trading (Article 184 of the Consolidated Law on Finance)
- Market manipulation (Article 185 of the Consolidated Law on Finance)

By way of example, the crime of insider trading could occur in the relations and information flows with Head Office or Headquarter, and specifically in the case of disclosure of precise information, not previously made public on the market, directly or indirectly, dealing with one or more financial

instruments, in order to have a significant influence on the price of such financial instruments or the price of the related derivative instruments.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Internal Operation and Management Authorization
- Financial Crime Policy
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Banking Business Manual
- Compliance Policy
- Compliance Charter
- Conflict of interest Policy
- Whistleblowing Policy
- Gifts and Entertainment Policy
- DAC 6 Procedure
- AML & Compliance Committee Charter
- Client Relationship Acceptance Committee Charter
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.3 Managing relations with Business Partners and Financial Intermediaries

This Risk Activity concerns processes related to:

a) identification and selection of business partners;
b) monitoring the situation of similar local banks;
c) preparation, organisation and execution of the marketing plan.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Insider trading (Article 184 of the Consolidated Law on Finance)
- Market manipulation (Article 185 of the Consolidated Law on Finance)

By way of example, the criminal offence of market manipulation occurs when any person disseminates false information or sets up sham transactions or employs other devices likely to produce a significant alteration in the price of the financial instruments listed in Article 182 of the Consolidated Law referred to in the introduction.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Anti Internal Fraud Policy
- Financial Crime Policy
- AML-CTF Due Diligence and Client Onboarding Procedure
- Conflict of interest Policy
- Internal Operation and Management Authorization
- Complaint handling procedure
- Banking Business Manual
- International Settlement and Trade Finance Operation Manual
- Gifts and Entertainment Policy
- Credit Manual
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.4 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;
c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Insider trading (Article 184 of the Consolidated Law on Finance)
- Market manipulation (Article 185 of the Consolidated Law on Finance)

By way of example, this offense could occur if the Branch uses restricted information, pertaining to

the business decisions of the Branch's customers, which became known during the preliminary investigation and/or information acquisition stage to analyze the loan application.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Market Abuse Policy
- Banking Business Manual
- Charter of Credit Committee
- CIB Business Manual
- Credit Manual
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Anti Internal Fraud Policy
- Complaint handling procedure
- Conflict of interest Policy
- CRS procedure
- Dac-6 procedure
- Financial Accounting Manual
- Financial Crime Policy
- General Governance Policy
- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- Procedure for Assessment and Approval of New Product
- Suspicious Transaction Reporting procedure
- Tax Affair Management Procedure
- Treasury manual
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of members of the "Deal Team," a restricted group of people who from time to time are in possession of restricted information;

2. establishment and maintenance of appropriate information barriers;
3. adoption and updating of the Insider List and related controls;
4. controls of completeness, correctness and accuracy of information transmitted regarding market abuse to Headquarter and/or Head Offices;
5. clear identification of the people/departments in charge of portfolio management;
6. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
7. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
8. staff awareness activities in the areas of the Branch's operations.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 25-sexies "Market abuse offences", the following should be noted:

1. for each transaction, the Deal Team must be registered in a special list ("Insider List"), constantly updated, which must contain the name of the project and the names of all staff members involved in the transaction;
2. staff members included on the Insider List are required to provide written confirmation of such inclusion, as well as declare that they undertake to comply with the relevant discipline and are aware of the relevant sanctions;
3. in the event that a staff member is potentially in possession of Restricted Information but is not on the Insider List, it is his or her personal responsibility to promptly inform the department that originated the transaction and the Legal & Compliance Department of this situation;
4. the Insider Lists are kept in special segregated folders;
5. on a semi-annual basis, staff members are required to complete and submit to the Legal & Compliance Department a report on the transactions conducted for appropriate verification in compliance with the Market Abuse Policy;
6. the Branch shall promptly report to CONSOB any transactions made by any of its staff members that it may reasonably consider suspicious in terms of potential confidential or privileged information or potential market abuse.

NINTH SECTION - WORKPLACE HEALTH AND SAFETY OFFENCES

1.1. Introduction

Article 25-septies of the Decree includes in the list of the Predicate offences giving rise to the liability of Entities the offences of unintentional killing (manslaughter) and of unintentionally causing grievous bodily injury where such offences are committed through violation of accident prevention and workplace health and safety rules.

The Consolidated Law on protection of health and safety in the workplace (Legislative Decree no. 81 of 9 April 2008), reorganized in a coherent framework the large number of previous legislative acts governing this area.
The purpose of the above legal provisions is to provide more effective means of prevention and punishment, in the light of the spike in the number of workplace accidents and of the need to safeguard the physical and mental wellbeing of workers and the safety of workplaces.
The two types of offences included in this Section regard respectively death or serious or grievous bodily harm, caused culpably.
Serious bodily injury indicates a condition which endangers the life of the injured person, or causes incapacity to attend to normal activities for a period exceeding forty days, or an injury which results in the permanent weakening of a sense or an organ; grievous bodily injury indicates a disease that is certainly or probably incurable;; the loss of a sense, a limb, a mutilation that renders the limb unserviceable, the loss of an organ or the capacity to procreate, permanent impairment of the power of speech.
According to Article 25-septies of the Decree, to give rise to the Entity's liability, both conducts must be characterised by violation of workplace accident prevention and health and safety protection regulations.
Various legal provisions cover this area, most of which have been since absorbed by the Consolidated Law on the protection of workplace health and safety, which repealed many of the previous special laws, among which we should mention: Presidential Decree no. 547 of 27.4.1955 on accident prevention; Presidential Decree no. 303 of 19.3.1956 on workplace hygiene; Legislative Decree no. 626 of 19.9.1994 which contained general provisions on the protection of workers' health and safety; and Legislative Decree no. 494 of 14.8.1996 on construction site safety.
The specific prevention requirements set out in sector legislation are complemented by the more general provision of Article 2087 of the Civil code, which requires employers to set in place measures to protect the physical and mental health of workers having regard to the characteristics of the work, the workers' experience and the techniques employed.
Lastly, it should be noted that according to case law the employer may also be liable for the offences in question where the injured person is not a worker but a third party, provided that his presence at the workplace at the time of the accident was neither anomalous nor exceptional.

Specifically, the offenses of manslaughter and grievous or very grievous bodily harm committed in violation of accident prevention and occupational hygiene and health protection regulations, covered in Article 25-septies of the Decree, include:

- **Manslaughter (Article 589 of the Criminal Code)**: anyone who culpably causes the death of a person is liable for this offense. An aggravating circumstance is having committed the act in violation of the rules for the prevention of accidents at work.

- **Negligent personal injury (Art. 590 Penal Code)**: anyone who negligently causes personal injury to another person is liable for this offense. It is an aggravating circumstance to have committed the act with violation of the rules for the prevention of accidents at work.

1.2. General rules of conduct

The Branch promotes a health and safety workplace.
The Branch is committed to providing for the health and safety of all employees and to maintaining standards at least equal to the best practice in the banking industry. However, it is the implicit responsibility of every member of staff to exercise responsibility and to do all possible to prevent injury to themselves and others by observing all safety regulations and by reporting potential dangers to the General Managers, without delay.
The Branch is committed to ensure so far as is reasonably practicable the health, safety and welfare at work of all its employees. This is a management responsibility equivalent to that of any other management function.

For a health and safety risk prevention and protection system to be effective and successful, it is vital that employees can contribute to establishing and maintaining a safe system of work. However, the Branch accepts that it has the primary responsibility for health and safety at work.

The Branch has appointed the persons with responsibility for first aid. The Branch has also prepared two first aider packs in the cafeteria areas.

In the event of an accident or illness occurring, the employees should contact the General Administration Department, give their name, location and brief details of the problem.

All accidents must be reported to the General Managers and the General Administration Department will record relevant details in the 'Accident Record' and take the necessary action to prevent a recurrence.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of occupational health and safety crimes being carried out is greatest generally concern the occupational health and safety management.

1.3.1 Occupational health and safety management

This Risk Activity concerns processes related to compliance with any type of activity aimed at

developing and ensuring a system of prevention and protection of workplace risks, in compliance with the provisions of Legislative Decree No. 81/2008 as amended:

a) organisation of roles and activities related to the protection of Health and Safety at Work;
b) management of risk assessment activities and preparation of the consequent prevention and protection measures;
c) management of emergencies;
d) information, training and involvement of workers in occupational Health and Safety;
e) management of health surveillance;
f) detection, recording and management of accidents and incidents.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Manslaughter (Article 589 of the Criminal Code)
- Negligent personal injury (Art. 590 Penal Code)

By way of example, this kind of offences could occur in the case where the negligent violation of occupational health and safety protection regulations results in an occupational accident that causes the death of a Branch employee, or as, for example, in the case of very serious bodily injury as a result of a fire that started on the Branch offices' premises due to a short circuit in the computer system, in connection with which the persons in charge of the system had negligently failed to carry out periodic functional and safety checks.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- DVR - Documento sulla Valutazione dei Rischi
- Code of Ethics
- Code of Conduct
- Staff Handbook
- Internal Operation and Management Authorization
- General Governance Policy
- Whistleblowing Policy

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. formal identification of persons in charge of occupational safety roles and responsibilities (Prevention and Protection Manager, Competent Doctor, workers in charge of applying fire

prevention and evacuation measures, etc.);

2. formalization of a “Documento di Valutazione die Rischi” (DVR) in accordance with the provisions of current preventive regulations;
3. preparation of emergency plans and evacuation plans;
4. conduct and tracking of health surveillance visits (new hires, periodic visits);
5. definition of rules for the detection, recording and investigation of accidents, incidents and near misses;
6. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
7. appropriate system for sanctioning non-compliance with the measures specified in the Model;
8. training activities on safety in the workplace.

TENTH SECTION - CRIMES CONCERNING RECEIPT OF STOLEN GOODS, MONEY LAUNDERING AND USE OF MONEY, GOODS OR BENEFITS OF UNLAWFUL ORIGIN, AS WELL AS SELF-LAUNDERING

1.1. Introduction

Article 25-octies of Legislative Decree no. 231/01 provides for the administrative liability of the Entity in the case of crimes concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering.

The legislation on the administrative liability of Entities in these crimes aims to prevent and combat more effectively the phenomenon of the introduction into lawful economic circuits of money, goods or other assets which are the proceeds of crime, as this hinders the activities of the justice system in detecting offences and prosecuting offenders, and in general damages the economic order, market integrity and free competition, by reason of the unfair competitive advantage enjoyed by those operators who have at their disposal financial resources of unlawful origin.

Still for the purpose of combating money laundering and of the financing of terrorism, within the said perimeter of the anti-Money Laundering Decree shall be considered as included all the laws and regulation and provisions concerning the banking and financial business activity and sector that establishes specific requirements for banks, financial intermediaries, and other specified obliged subjects (appropriate checks on customers; recording and storage of transaction documents; reporting of any suspicious transactions; notification of any infringements of the prohibitions concerning cash and bearer securities; reporting by the Entity’s control of any infringements identified) because they are measures provided for fighting, in a broader sense (so inclusive of all the illegal conducts are qualified as predicated Offences), the money laundering that is a Predicated Offence and constitute liability for the Branch.

Infringement of said obligations cannot be qualified as, and does not give always rise to, Entity’s

administrative liability under Legislative Decree no. 231/2001, since such offences are not included in the list of the so-called Predicate offences, but said infringement is in any case punished pursuant to the anti-money laundering Decree, to ensure compliance in all cases with the fundamental principles of in-depth knowledge of customers and the traceability of transactions, to avoid any danger that financial intermediaries might be unwittingly involved in illegal activities.

It should be noted that if the Branch operator fails to perform his obligations being fully aware of the illegal origin of the goods subject of the transactions, he could be indicted for such offences, and consequently the Branch might incur administrative liability under Legislative Decree no. 231/2001.

The material subject of these offences can consist of any asset having appreciable economic value and which may be exchanged, concealed; transferred and/or changed, such as money, credit securities, means of payment, credit entitlements, precious metals/gems, tangible and intangible assets, rights and financial options in general. These goods or assets must originate from the crime, i.e. they must be the product (the result or benefit obtained by the offender by committing the crime), the proceeds (monetary gain or economic benefit obtained from the offence) or the price (amount paid to induce, instigate, or lead someone to commit the offence). In addition to the crimes typically aimed at the creation of illegal capital,(e.g.: extortion in office, bribery, embezzlement, fraud, bankruptcy crime, arms or drug trafficking, usury, fraud against EU funds, et cetera) and tax offences as provided by the L.D. No. 74/2000 could also give generate to proceeds which are then laundered or of self-laundering, not only for fraud - tax fraud too - (for ex., the use of invoices for non-existent transactions that result in a fictitious credit; VAT to be deducted) but also in the case in which the economic utility consequential to a crime consists in a mere tax saving to be qualified as illicit as subsequent and/or due (because of/related) to the non-disbursement of money originating from legal activities, (for example, failing to report or misreporting the income for amounts above the threshold of criminal relevance).

A third party not involved in the original crime that generates illegal proceeds and who receives them from the original offender (or from others, however knowing of the illegal origin) to perform conduct thereupon provided for by the said crimes shall be answerable to the crimes of receipt, laundering or illegal reuse of stolen goods.

A party who provided any type of moral or material causal contribution to the commission of the original offence for example determining or strengthening the criminal intent of the original offender with the promise, even before the commission of offence, his help in the recycling/using the proceeds could instead be answerable to conspiracy in the crime that generated the illegal proceeds and, consequentially, also in the subsequent crime of self-laundering, should he carry out the conduct.

The crime of self-laundering, unlike as prescribed for crimes of money laundering and of unlawful use, requires that the conduct be characterized by methods suitable for the actual masking of the true criminal origin of the goods and is often related to tax evasion conducts; the interpretation of the most innovative aspects of the law- that is to say requirement of the actual hindrance and the

condition of non-liability to punishment of the self-launderer for personnel use (which would again seem to be excluded if the original offence and the reuse take place in the performance of a business activity) – shall necessarily refer to the jurisprudential applications of the new crime.
As to the subjective element, as already stated, the offences in question must be marked by awareness of the fact that the goods in question are the proceeds of crime. According to a particularly strict interpretation, the offence may also occur if the person dealt with the goods while harboring suspicions as to their illegal origin, accepting such risk ("dolus eventualis" – that is a willful conduct accepting the risk of committing a crime - or indirect intention). With reference to banking operations, it should be noted that the presence of anomaly indicators or anomalous conducts as set out in the measures and in the patterns issued by the competent Authorities (as concerns financial intermediaries, by the Bank of Italy and by the UIF (Finance Intelligence Unit) in specific concrete situations might, if the particularly strict interpretation mentioned above is adopted, be considered as a serious and univocal objective circumstance which should give rise to doubts as to the illegal origin of the goods.

Specifically, Crimes concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering, set out in Article 25-octies of the Decree, include:

- **Receiving stolen goods (Art. 648 of the Criminal Code)**: anyone who, in order to procure a profit for himself or others, purchases, receives or conceals money or things resulting from any crime, or in any way meddles in having them purchased, received or concealed, shall be liable for this crime, outside the cases of complicity.
- **Money laundering (Art. 648-bis of the Criminal Code):** anyone who replaces or transfers money, goods or other utilities resulting from a crime, or carries out other transactions in relation to them, in such a way as to hinder the identification of their criminal origin, is liable for this crime, apart from cases of complicity in the crime.
- **Use of money, goods or utilities of unlawful origin (Art. 648-ter of the Criminal Code)**: anyone who, outside the cases of complicity in the crime and the cases provided for in Articles 648 and 648-bis, uses money, goods or other utilities resulting from crime in economic or financial activities is liable for this crime.
- **Self-money laundering (Article 648-ter.1 of the Criminal Code)**: anyone who, having committed or conspired to commit a crime, employs, substitutes, transfers, in economic, financial, entrepreneurial or speculative activities, the money, goods or other utilities resulting from the commission of such crime, in such a way as to concretely hinder the identification of their criminal origin, shall be liable for this crime.

1.2. General rules of conduct

As a commercial Branch that offers customers with diversified financial products and services, the branch takes serious attention to its obligation to collaborate with governments, international organization and other members of the financial services industry to help close off the channel that money lauder use committing money laundering.

It is required of all employees of the Branch to act in accordance with applicable law and protect the Branch from money laundering.

The Branch has established specific policies and procedures that all employees must follow.

It is mandatory for the employee to participate in the special ongoing training programs organized by the Branch in order to be able to recognize operations, which may be related to money laundering and to know he proceed in such cases as well as, more generally, be aware of the AML/CFT obligations.

According to the legislative provisions, the Branch is committed to file suspicious-activity reports with competent authorities regarding suspected operations.

The Branch in also bound by an obligation to provide without delay to the UIF and other competent Authorities, at its request or subsequent to a suspicious transaction reporting, any information. The branch has policies and procedures for reporting suspicious activity to or perform any due and/or useful cooperation with competent authorities.

Every employee is required to report all cases, where an employee of the Branch suspects or has reasonable grounds to believe that a customer might have engaged in indictable offences or AML/CFT, must promptly be reported to the MLRO of the Branch. The officer will decide whether reporting to competent authorities is required.

Every employee shall not disclose to the customer concerned or to other third person the fact that information is being reported or provided to the competent authorities or that money laundering or terrorist financing investigation by the UIF is being or may be carried out,

The Branch carries on its business in full compliance with the current anti-money laundering legislation and the provisions issued by the competent Authorities, to this end undertaking to refuse to carry out suspicious transactions in terms of fairness and transparency.

In general, the Branch undertakes:

- to verify in advance, with professional diligence, the information available on commercial counterparties, professionals and external consultants, in order to assess their respectability and the legitimacy of their business, before establishing business relationships;
- to acquire during the customer due diligence on customers any AML data and/or information that is obligatory and/or useful, also for the potential use of AML data for tax purposes and verification, in order to be compliant with all declarative obligations related to and arising/originated from the tax international cooperation agreement;
- to operate in such a way as to avoid any implication in suitable operations, even potentially,

to encourage money laundering, acting in full compliance with anti-money laundering legislation.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Crimes concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering is generally higher concern the following:

1. Operational cost management
2. Customer account management and monitoring
3. Customer relationships
4. Accounting
5. Public Administration relationship
6. Banking Supervisory Authorities relationship
7. Procurement of goods and services and appointment of professional assignments
8. Management of gifts
9. Management of payments
10. Staff selection, recruitment and management
11. Credit-related activities
12. Management of litigation and out-of-court procedures
13. Data and Information Systems Management
14. Managing relations with Business Partners and Financial Intermediaries
15. Occupational Health and Safety Management
16. Tax management
17. Waste production, discharges, air emissions and soil pollution
18. Marketing and sales strategies

1.3.1 Operational cost management

This Risk Activity mainly concerns processes related to the review and approval of daily operational costs.

The General Manager is ultimately responsible for the operating expense management, all daily expenses shall be reviewed and approved by the General Manager but the expenses above 15.000€ are approved by the Financial Affairs Committee of the Branch.

The types of crime that are abstractly applicable and the related methods of committing them are

listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code

By way of example, the offense of money laundering could occur if the employee through artifice or deception includes expenses not actually incurred in order to allow illicit capital to enter the economic circle.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Operating Expense Management Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Financial Accounting Manual
- Centralized Procurement Rules
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Anti Internal Fraud Policy
- Credit Manual
- Banking Business Manual
- Gift and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Customer account management and monitoring

This Risk Activity concerns processes related to:

a) customer account profile management
b) account opening/closing;
c) management of dormant customers, dormant accounts and possible re-activation;
d) deviations from standard tariffs;
e) monitoring of accounts and customer information;
f) RMA exchange operation with the correspondent bank;

g) management of account or other product usage anomalies.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code

By way of example, this offence occurs when a customer replaces, or transfers money coming from a crime or carries out other transactions involving such money in such a way as to hinder the identification of their criminal source.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Financial Crime Policy
- Banking business manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Anti Internal Fraud Policy
- BRAINS Manual
- Code of Ethics
- Code of Conduct
- Anti Internal Fraud Policy

1.3.3 Customer relationship

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;

e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code

By way of example, the offences under consideration could occur in the event that the Head of the Banking Department carries out a suspicious transaction requested by a customer by failing to send the appropriate STR report to the Money Laundering Reporting Officer for Suspicious Transactions (MLRO).

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- AML-CTF Due Diligence and Client Onboarding Procedure
- AML & Compliance Committee Charter
- Suspicious Transaction Reporting Procedure
- Customer Due Diligence Archiving Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Complaint handling Procedure
- Credit Manual
- Financial Crime Policy
- Anti Internal Fraud Policy.
- CIB Business Manual
- PEP Procedure
- BRAINS Manual
- Banking Business Manual
- DAC-6 procedure

- CRS procedure
- FATCA Procedure
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.4 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;
c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;
f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Headquarter.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code

By way of example, the type of offense under consideration could be configured by inserting fake suppliers or customers in the management and accounting system and transferring money from illegal activity, in order to facilitate its re-entry into the economic circuit, obtaining a monetary advantage from carrying out this activity.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Accounting Manual
- Credit Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Third Party Management
- Anti Internal Fraud Policy.
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.5 Public Administration relationship

This Risk Activity concerns processes related to:

a) management of relations with Chambers of Commerce;
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding hygiene and safety and/or authorisations, permits, concessions;
d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;
e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police, Guardia di Finanza);
h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g., INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)

- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code

By way of example, the offense of money laundering could take place in the event that part of the salary is paid to employees in the form of reimbursement for business trips, in order to avoid the payment of part of the contributions due to the public institutions related to the salary, and the consequent utilization of these illicit amount to fulfill a contract with an outsourcer of the Branch.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Financial Crime Policy
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Training Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.6 Banking Supervisory Authorities relationship

This Risk Activity concerns processes related to:

a) processing/transmission of occasional or periodic reports to the Supervisory Authorities;
b) requests/applications for licenses and/or authorisations;
c) feedback and compliance with applications/requests from the Supervisory Authorities;
d) management of relations with the Officials of the Supervisory Authorities during their inspection visits;
e) monitoring remediation actions and reporting/informing the Supervisory Authority.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)

- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code

By way of example, the offense could occur if a person, in order to hinder the exercise of supervisory functions, replaces or transfers money, goods or other utilities derived from crime in such a way as to hinder the identification of their criminal origin.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Suspicious transaction reporting procedure
- AUI and SARA reporting procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- CRS procedure
- FATCA procedure
- Procedure for management of external inspections
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.7 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code).

.

By way of illustration, the crime of money laundering could be realized by the use of consulting services for non existent services in order to conceal the real illicit origin of the money or to facilitate, through the performance of tax offenses, the laundering of such illicitly produced capital or in having the same purpose of concealing capital of illicit origin through the use of banking and financial services and/or through the use of products or services of the Branch.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Centralized Procurement Rules
- Financial Crime Policy
- Operating Expense Management Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- General Governance Policy of ICBC Milan Branch
- Policy on the Management of the External Legal Advisors
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Conflict of interest Policy
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.8 Management of gifts

This Risk Activity mainly concerns processes related to:

a) Management of liberal initiatives;

b) Management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code).

By way of example, the crime could occur if the Branch launders money from illegal activities by using such funds to pay gifts or entertainment expenses to third parties.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Centralized Procurement Rules
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.9 Management of payments

This Risk Activity concerns processes related to the management of the payment of sales/goods/services actually rendered/received.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)

- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offense could occur if the Branch pays its suppliers money from crime in such a way as to hinder the identification of its criminal origin.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Suspicious Transaction Reporting Procedure
- Centralized Procurement Rules
- Operating Expense Management Rules
- Financial Affairs and Centralized Procurement Management Committee
- Financial Crime Policy
- Banking Business Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Anti-Internal Fraud Policy
- Third-party Management Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.10 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;

m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this crime could occur if the Branch launders money from illegal activities by employing these assets to pay salaries of employees.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Rights and duties of the employees' disciplinary measures
- HR Management System Instructions
- Measures Staff Recruitment
- Employer Personal Data Processing Policy
- Performance Appraisal Guidelines
- Training Policy
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Operating Expense Management Rules
- Anti-Internal Fraud Policy
- Conflict of interest Policy
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.11 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;

c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offense could occur if a Branch employee allowed a client company to keep its account active, even where the necessary AML controls could not be carried out, in order to ensure that large amounts of money passed through the Branch's bank accounts.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Financial Accounting Manual
- Anti Internal Fraud Policy
- Banking Business Manual
- Charter of Credit Committee
- CIB Business Manual
- Credit Manual
- CRS procedure
- Dac-6 procedure
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Conflict of interest Policy
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Code of Conduct
- Code of Ethics

1.3.12 Management of litigation and out-of-court procedures

This Risk Activity concerns processes related to:

a) complaints management;
b) management of active and passive judicial/out-of-court disputes (civil, criminal, administrative, labour law - debt collection) also with the external professional's assistance;
c) managing and monitoring settlement agreements.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offense could occur if the Branch, for the management of a judicial/judicial dispute involving it, entrusts the practice to an outside professional and makes fee payments through the use of money from illegal activity.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Legal function working manual
- Policy on the Management of External Legal Advisor
- General Governance Policy of ICBC Milan Branch
- Complaint handling Procedure
- Anti Internal Fraud Policy
- Internal Operation and Management Authorization
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.13 Data and Information Systems Management

This Risk Activity concerns processes related to:

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;

b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this crime could be committed by falsifying the management system by entering fictitious expenses in the branch's accounts and transferring money from illicit activities in order to facilitate their re-entry into the economic circuit, thereby obtaining a monetary advantage from the performance of such activity.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Guidelines on System and Network Management
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Rules of IT General Management
- Information Security Policy
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- IT Governance-Equipment Management

- Measures of Information and Information System Security Management
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- Security Management-Network&System Security
- Technical Specifications for Security Technique for Network System
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct

1.3.14 Managing relations with Business Partners and Financial Intermediaries

This Risk Activity concerns processes related to:

a) identification and selection of business partners;
b) monitoring the situation of similar local banks;
c) preparation, organisation and execution of the marketing plan.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this type of crime could occur if the Branch launders money from illicit activities by employing these availabilities for the payment of fees to business partners/financial intermediaries or by making payments to them for fictitious arrangements or for an amount greater than the amount actually due so as to obstruct the criminal origin of the money employed.
The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- AML-CTF Due Diligence and Client Onboarding Procedure
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Internal Operation and Management Authorization

- International Settlement and Trade Finance Operation Manual
- Anti Internal Fraud Policy

- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.15 Occupational Health and Safety Management

This Risk Activity concerns processes related to compliance with any type of activity aimed at developing and ensuring a system of prevention and protection of workplace risks, in compliance with the provisions of Legislative Decree No. 81/2008 as amended:

a) organisation of roles and activities related to the protection of Health and Safety at Work;
b) management of risk assessment activities and preparation of the consequent prevention and protection measures;
c) management of emergencies;
d) information, training and involvement of workers in occupational Health and Safety;
e) management of health surveillance;
f) detection, recording and management of accidents and incidents.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offence could occur if the Branch launders and employs money from illicit activities by obtaining undue expense savings through the omission, including negligence, of precautions or defenses against accidents at work, such as avoiding renewing safety measures to prevent fires or other types of accidents.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct
- Staff Handbook
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Whistleblowing Policy

1.3.16 Tax management

This Risk Activity concerns processes related to:

a) drafting, approving and sending tax declarations or payment forms;
b) direct and indirect taxes payments;
c) management of active/passive invoicing;
d) storage of accounting records.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offence could occur if the Branch presents tax documentation containing less than actual assets, or fictitious liabilities, which could form the basis for the commission of the crime of self-laundering.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Suspicious Transaction Reporting procedure
- Financial Accounting Manual
- Tax Affairs Management Procedure
- Treasury Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Dac-6 procedure
- CRS Procedure
- FATCA Procedure

- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.17 Waste production, discharges, air emissions and soil pollution

This Risk Activity concerns processes related to:

a) waste identification and classification process;
b) collection and management of temporary storage of waste;
c) purchasing and supplier management;
d) facilities management (air conditioning, water discharges, etc.);
e) management of cleaning services.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offence could occur if the Branch launders and employs money from illicit activities by obtaining undue expense savings through the commission of contraventions punishable by the Environmental Code, pertaining to the improper management and disposal of waste.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- ESG strategy action plan
- Code of Ethics
- Code of Conduct
- Staff handbook
- Third Party Management Procedure

1.3.18 Marketing and sales strategies

This Risk Activity concerns processes related to:

a) promotion of the Branch's image on the Italian market;
b) development of marketing and sales strategies;
c) management of relations with prospects;
d) organisation of meetings with potential clients;
e) management of external reporting;
f) management of the proposition of new products, services or activities of the Branch (Definition of business needs; Preliminary investigation and evaluation of new products/services; Approval of new products/services).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Receipt of stolen goods (Article 648 of the Criminal Code)
- Money laundering (Article 648-bis of the Criminal Code)
- Use of money, goods or assets of illegal origin (Article 648-ter of the Criminal Code)
- Self-laundering (Article 648-ter.1 of the Criminal Code)

By way of example, this offence could occur if the Branch carries out operations to use, substitute or transfer in economic, financial, entrepreneurial or speculative activities, money, goods or other utilities from a crime committed in the context of promoting new products/services.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure

ICBC Milan Branch Business Processing Procedures of Financial Markets Business

- Procedure for Assessment and Approval of New Product
- Financial Accounting Manual
- Centralized Procurement Rules
- Anti Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Internal Operation and Management Authorization
- Treasury manual
- Dac-6 procedure
- CRS procedure

- Procedure on the management of external legal advisors
- Legal function working manual
- Tax Affair Management Procedure
- Code of Ethics
- Code of Conduct

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of the people/departments in charge of managing and monitoring customer accounts;
2. transparent and reconstructible decision-making processes over time regarding conditions stipulated with customers;
3. paper and/or electronic tracking of conditions stipulated with customers;
4. customer identification for anti-money laundering purposes;
5. correctness and completeness of the data surveyed updated in the registry in order to achieve timely and updated profiling of customers for anti-money laundering purposes;
6. definition of controls and related reporting on potentially anomalous transactions;
7. periodic updating of information on customer relationships in order in order to enable a constant assessment of their money laundering risk profile;
8. clear identification of the people in charge of managing the accounts
9. monitoring of AML and KYC compliance in all existing and potential customer relationships;
10. clear identification of the people/departments in charge of the purchase of goods and services and the awarding of professional appointments;
11. accurate verification of necessary qualifications, skills and requirements of suppliers;
12. periodic monitoring of supplier qualification;
13. properly formalized requests for proposals addressed to suppliers;
14. periodic monitoring of suppliers' performance;
15. archiving of supplier contract documentation;
16. tracking of all IT events, problems and changes to the Branch IT system;
17. periodic monitoring/control activities on the operations of the Branch including by the Surveillance Body;
18. appropriate system for sanctioning non-compliance with the measures specified in the Model;
19. staff awareness activities in the areas of operation of the Branch.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 25-octies " Crimes concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as

self-laundering", the following should be noted:

1. no services may be provided prior to the identification and verification of the identity of the customer, of the beneficial owner and executors;
2. the front office Departments provide for the identification and verification of the identity of customers before the opening of an account and performs "Customer Due Diligence (CDD)" in accordance with the anti-money laundering and anti-terrorism regulations in force;
3. the client's money laundering risk classification shall be updated regularly by the front office Departments in accordance with review cycles or due to potential changes that may impact the client's risk assessment;
4. for each outgoing payment transaction by low or medium risk customers holding a bank account with the Branch, when the amount is EUR 100,000 or more, the Banking Department must mandatorily obtain the written approval of a member of the Legal & Compliance Department on the relevant transfer voucher before executing such transaction.

   In the case of outgoing payment transactions of high risk customers, when the amount is EUR 20,000 or more, the Banking Department must mandatorily obtain the approval of a member of the Legal & Compliance Department. Where the amount is EUR 100,000 or more, a second validation by the Head of the Legal & Compliance Department or his deputy is required.
5. the Branch adopts and maintains the Single Computer Archive (AUI) and periodically reports aggregate transaction data (S.A.R.A. reporting) to the FIU;
6. General Management puts in place all necessary actions to ensure the effectiveness of the AML control system;
7. the Legal & Compliance department reports annually to the Bank of Italy through the AML Annual Report including the AML Self-Assessment;
8. the AML & Compliance Committee reports to General Management (and Headquarter, to whom the minutes of each meeting are sent) on the overall status of the Branch's AML and suspicious transaction reporting activities;
9. any anomalous suspicious money laundering behavior should be reported first to the head of the relevant Department and, if applicable, immediately to the Money Laundering Reporting Officer. The Legal and Compliance Department or the MLRO, in case of escalation, will make the necessary investigation and possible reporting to the local Financial Intelligence Unit (FIU);

ELEVENTH SECTION - CRIMES RELATING TO NON-CASH PAYMENT INSTRUMENTS

1.1. Introduction

This Section covers the offenses provided for in Article 25.octies.1 of the Decree, added by

Legislative Decree 184/2021, i.e., the offenses provided for on the subject of non-cash payment instruments.

Legislative Decree No. 184/2021 "Implementation of Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment" amended the heading and subparagraphs of Art. 493-ter of Royal Decree No. 1398 of October 19, 1930, inserted into the Criminal Code Art. 493-quater (Possession and dissemination of computer equipment, devices or programs aimed at committing offenses regarding non-cash means of payment) and expanded the offenses covered by the Decree with the insertion, after Article 25-octies, of Art. 25-octies.1.

It incurs the crimes covered by Art.25-octies.1, for the protection of assets as well as the proper circulation of credit:

- who uses credit card not being a cardholder having stolen it;
- who uses credit card not being its holder even having only found it;
- whoever forges credit cards;
- who surrenders forged credit cards;
- whoever puts counterfeit credit cards into circulation;
- whoever procures for himself or others an unjust profit by altering the operation of a computer system.

The crime is consummated when the cards or computer programs are used regardless of whether or not there has been a gain.

Specifically, the offenses involving non-cash payment instruments covered in Article 25-octies.1 of the Decree include:

- **Misuse and forgery of non-cash payment instruments (Article 493-ter of the Criminal Code):** anyone who, in order to make a profit for himself or others, unduly uses, not being the holder, credit or payment cards, or any other similar document enabling the withdrawal of cash or the purchase of goods or the provision of services or, in any case, any other payment instrument other than cash, or anyone who, in order to make a profit for himself or others forges or alters the instruments or documents referred to above, or possesses, disposes of or acquires such instruments or documents of illicit origin or otherwise forged or altered, as well as payment orders produced with them.
- **Possession and dissemination of equipment, devices or computer programs aimed at committing crimes regarding non-cash payment instruments (Article 493-quater of the Criminal Code)**: anyone who, unless the fact constitutes a more serious crime, in order to make use of them or to allow others to use them in the commission of crimes regarding non-cash payment instruments, produces, imports, exports, sells, transports, distributes, makes available or in any way procures for himself or others equipment, devices or computer programs that, due to technical-constructive or design characteristics, are primarily

constructed to commit such crimes, or are specifically adapted for the same purpose.

- **Computer fraud aggravated by the realization of a transfer of money, monetary value or virtual currency (Art. 640-ter of the Criminal Code)**: anyone who, by altering in any way the operation of a computer or telematic system or intervening without the right in any manner on data, information or programs contained in a computer or telematic system or pertaining to it, procures for himself or others an unfair profit to the detriment of others is liable for this crime.
- **Fraudulent transfer of valuables (Art. 512-bis of the Criminal Code):** anyone who, unless the fact constitutes a more serious crime, fictitiously attributes to others the ownership or availability of money goods or other utilities in order to evade the provisions of the law on property prevention measures or smuggling or to facilitate the commission of one of the crimes referred to in Articles 648 648-bis and 648-ter of the Penal Code shall be liable for this crime.

1.2. General rules of conduct

Risk Activities must be carried out in compliance with applicable laws, the rules set forth in this Model and, also but not limited to, the provisions of the Code of Ethics and the Code of Conduct, an expression of the values and policies of the Branch.

Actions, operations carried out on behalf of the Branch must be guided by the principles of:

- separation of roles and responsibilities within the Branch;
- fairness, completeness and transparency of information;
- formal and substantive legitimacy;

in accordance with current regulations and according to established procedures.

Branch employees involved in the management of Risk Activities are required, in order to prevent the occurrence of the offenses in question, to comply with the following general principles of conduct:

- to abstain from engaging in conduct such as to integrate the types of offenses considered above (Article 25-octies.1 of the Decree);
- to abstain from engaging in or adopting behaviors and/or acts that are prodromal to the subsequent realization of the types of offenses indicated in this Section.

Recipients of the Model are required to promptly report any potential forgery and undue use of non-cash financial instruments of which they become aware.

The risk of crime under Article 25-octies.1 is mitigated by procedural and enforcement limitations and continuous internal controls and monitoring, as well as by internal rules and ethical principles of behavior.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, in spite of the Branch's limited operation of non-cash payment instruments, the activities in which the risk of unlawful conduct in relations with such crimes is generally higher concern the following:

1. Customer account management and monitoring
2. Data and Information Systems Management
3. Staff selection, recruitment and management

1.3.1 Customer account management and monitoring

This Risk Activity concerns processes related to:

a) customer account profile management
b) account opening/closing;
c) management of dormant customers, dormant accounts and possible re-activation;
d) deviations from standard tariffs;
e) monitoring of accounts and customer information;
f) RMA exchange operation with the correspondent bank;
g) management of account or other product usage anomalies.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Misuse and forgery of non-cash payment instruments (Article 493-ter of the Criminal Code)
- Possession and dissemination of equipment, devices or computer programs aimed at committing crimes regarding non-cash payment instruments (Article 493-quater of the Criminal Code):
- Computer fraud aggravated by the realization of a transfer of money, monetary value or virtual currency (Art. 640-ter of the Criminal Code

By way of example, the offense could occur if the Branch omits or improperly performs the preliminary checks necessary in order to grant a customer the use of E-BANKING TOKEN. Banking Department has to enter the serial number of the TOKEN into the FOVA system for management and is also in charge of setting up and maintaining the system's parameter table, scheduling of accounting items, utilisation and stock management.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- AML-CTF Due Diligence and Client Onboarding Procedure
- AML & Compliance Committee Charter
- Suspicious Transaction Reporting Procedure
- Financial Crime Policy
- Anti Internal Fraud Policy
- BRAINS Manual
- Banking business manual
- Charter of Credit Committee
- Credit Manual
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Conflict of interest Policy
- Whistleblowing Policy
- Gifts and Entertainment Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.2 Data and Information System Management

This Risk Activity concerns processes related to:

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;
b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Possession and dissemination of equipment, devices or computer programs aimed at committing crimes regarding non-cash payment instruments (Article 493-quater of the Criminal Code)

- Computer fraud aggravated by the realization of a transfer of money, monetary value or virtual currency (Art. 640-ter of the Criminal Code)

By way of example, these offenses could occur if the Branch uses computer programs that, due to technical or design characteristics, are primarily constructed to falsify, alter, or allow the misuse of non-cash payment instruments.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Guidelines on System and Network Management
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Rules of IT General Management
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- IT Governance-Equipment Management
- Measures of Information and Information System Security Management
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- Information Security Policy
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- Security Management-Network&System Security
- Technical Specifications for Security Technique for Network System
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.3 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;

c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Misuse and forgery of non-cash payment instruments (Article 493-ter of the Criminal Code)

By way of example, the offense could occur if the Branch provides employees with counterfeit credit cards to be used for expenses to be incurred during travel.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Operating Expense Management Rules
- HR Management System Instructions March 2023
- Code of Conduct
- Code of Ethics
- Staff Handbook
- Measures Staff Recruitment
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Employer Personal Data Processing Policy
- Rights and duties of the employees' disciplinary measures
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Internal Fraud Policy
- Anti-Bribery and Corruption Policy

- Gifts and Entertainment Policy
- Third-party Management Procedure
- Performance Appraisal Guidelines
- Training Policy

1.4. Mitigation factors

The control system to guard the processes described above essentially involves technological and IT safeguards. The Risk Activities highlighted above are effectively guarded with the implementation of the IT and AML security measures referred to herein in full (Second and Tenth Sections of the Model).

The Branch has an Internet home banking platform for customers for whom PSD2 (Payment Services Directive 2015/2366) regulations apply, protected by a strong authentication system. The Branch does not have digital services managed through mobile applications nor does it operate ATMs.

Despite the Branch's limited operation of non-cash payment instruments, there are stringent authorization levels and specific rules to be followed, such as, for example, the controls carried out by the Banking Department in the area of payment orders.

In this context, the Banking Department:

1. checks payment orders received by banking.icbc@pec.it;
2. examines the notarised signature kept on file with the payment order signature; checks the validity of the identity document and the letter of indemnity
3. contacts the corporate customer to confirm the payment order;
4. after verification, use the "verified signature" "PEC TO PEC" stamps (if the order is received from the customer's pec) and sign the document;
5. complete the payment transaction and send the customer receipt generated the next day via the notification platform.

TWELFTH SECTION – CRIMES INVOLVING BREACH OF COPYRIGHT

1.1. Introduction

Article 25-novies of the Legislative Decree no.231/01 in order to strengthen the fight against intellectual property piracy and counter the serious economic damage it causes to authors and to the related industry – refers to offences set out in the copyright law (Law no. 633/1941).

Pursuant to Article 1 of Law no. 633/1941, intellectual works protected by copyright are those belonging to literature (including scientific and educational literature), music, the figurative arts, architecture, theatre, and film, irrespective of their form of expression. Computer software and data banks which by their choice of arrangement of materials constitute an intellectual creation of their

author are also ranked as literary works.
In general, the crimes occurs when any person, without being authorised, for any purpose and in any form, makes available to the public a protected intellectual work, or a part thereof, by placing it in a system of telecommunications networks through connections of any kind.
Is also punished the use of others' intellectual works by means of reproduction, transcription, dissemination in any form, placing for sale, placing on telecommunications networks, public performance or representation, creative uses such as translations, summaries, et cetera.
If the conduct is characterised by profit-making aims, the conduct is punished more severely.
Regarding the software and databases, the legislation punishes the conducts of unauthorized duplication and import, reproduction, distribution, sale, holding for commercial or business purposes (hence also for internal use within one's undertaking) and leasing, when such conducts concern software contained in media not bearing the SIAE mark (Italian Society of Authors and Publishers).
In addition, the legislation provides the crime of Abuses concerning audiovisual or literary works, failure to make communications or making false communications to SIAE and fraudulent unscrambling of restricted-access transmissions.

Specifically, Crimes involving breach of copyright, set out in Article 25-novies of the Decree, include:

- **Making available to the public, in a system of telematic networks, through connections of any kind, a protected intellectual work, or part of it (Article 171, Law No. 633/1941 paragraph 1 letter a) bis)**: anyone who, without having the right to do so, for any purpose and in any form whatsoever:
  a) reproduces, transcribes, performs in public, disseminates, sells or otherwise places on the market a work of others or reveals its content before it is made public, or introduces and places in circulation in the State copies produced abroad contrary to Italian law
  (a-bis) makes available to the public, by entering it into a system of telematic networks, through connections of any kind, a protected intellectual work, or part of it
  (b) represents, performs or recites in public or broadcasts, with or without variations or additions, a work of another person suitable for public performance or a musical composition. Representation or performance includes public showing of the cinematographic work, public performance of musical compositions included in cinematographic works and broadcasting by means of a loudspeaker operated in public;
  (c) performs the acts indicated in the preceding subparagraphs by means of one of the forms of elaboration provided for by this Act;
  (d) reproduces a greater number of copies or performs or plays a greater number of performances than he had a right to reproduce or play, respectively;
  (e) deleted;
  (f) in violation of Section 79, rebroadcasts by wire or by radio or records in phonogram discs

or other similar apparatuses the radio broadcasts or rebroadcasts or disposes of the phonogram discs or other apparatuses unduly recorded.

- **Unauthorised duplication, for profit, of computer programs; import, distribution, sale or possession for commercial or entrepreneurial purposes or rental of programs contained in media not marked by the SIAE; preparation of means for removing or circumventing the protection devices of computer programs (Art. 171-bis Law No. 633 /1941 paragraph)**: this offence is committed by anyone who unlawfully duplicates, for profit, computer programs or for the same purposes imports, distributes, sells, holds for commercial or entrepreneurial purposes or leases programs contained in media not marked by the SIAE or any means intended solely to allow or facilitate the arbitrary removal or functional circumvention of devices applied to protect a computer program.
- **Reproducing, transferring to another medium, distributing, communicating, presenting or demonstrating in public, the contents of a database; extracting or reusing the database; distributing, selling or leasing databases (Article 171-bis of Law No. 633/1941, paragraph 2)**: This offence is committed by any person who, in order to make a profit, on media not bearing the SIAE mark, reproduces, transfers to another medium, distributes, communicates, presents or demonstrates in public the contents of a database in breach of the provisions of Articles 64-quinquies and 64-sexies, or extracts or reuses the database in breach of the provisions of Articles 102-bis and 102-ter, or distributes, sells or rents out a database.
- **Unauthorised duplication, reproduction, transmission or dissemination in public by any process, in whole or in part, of intellectual works intended for the television, cinema, sale or rental of records, tapes or similar media or any other media containing phonograms or videograms of musical, cinematographic or audiovisual works assimilated or sequences of moving images literary, dramatic, scientific or didactic, musical or dramatic-musical, multimedia works, even if included in collective or composite works or databases; reproduction, duplication, transmission or unauthorised dissemination, sale or trade, transfer for any reason or unauthorised importation of more than fifty copies or specimens of works protected by copyright and related rights; introduction into a system of telematic networks, through connections of any kind, of an original work protected by copyright, or part of it (Art. 171-ter law no. 633 /1941)**: anyone who (if the act is committed for non-personal use)

  a) unlawfully duplicates, reproduces, transmits or disseminates in public by any process, in whole or in part, a work of art intended for the television, film, sale or rental circuit, discs, tapes or similar supports or any other support containing phonograms or videograms of musical, cinematographic or audiovisual works assimilated or sequences of moving images

  (b) unlawfully reproduces, transmits or disseminates in public, by any process, literary,

dramatic, scientific or educational, musical or dramatic-musical or multimedia works or parts thereof, even if they are included in collective or composite works or databases

(c) while not having participated in the duplication or reproduction, introduces into the territory of the State, holds for sale or distribution, or distributes, markets, rents or otherwise disposes of for any reason, projects in public, broadcasts by television by any process whatsoever, broadcasts by radio, or plays in public the unauthorised duplications or reproductions referred to in subparagraphs (a) and (b)

(d) holds for sale or distribution, markets, sells, rents, disposes of for any reason, projects in public, broadcasts by radio or television by any process, video cassettes, music cassettes, any medium containing phonograms or videograms of musical works cinematographic or audiovisual works or sequences of moving images, or any other medium for which, pursuant to this law, the affixing of a seal by the SIAE is prescribed, without such seal or with a counterfeit or altered seal;

e) in the absence of agreement with the lawful distributor, retransmits or broadcasts by any means whatsoever an encrypted service received by means of apparatuses or parts of apparatuses designed to decode conditional access transmissions

f) introduces into the territory of the State, holds for sale or distribution, distributes, sells, rents, transfers for any reason, commercially promotes, installs special decoding devices or elements that allow access to an encrypted service without payment of the due fee.

f-bis) manufactures, imports, distributes, sells, rents, transfers for any reason, advertises for sale or rent, or possesses for commercial purposes, equipment, products or components or provides services which have the predominant purpose or commercial use of circumventing effective technological measures referred to in Article 102-quater or are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of the aforesaid measures. Technological measures include those applied, or which remain, following the removal of such measures as a result of the voluntary initiative of the data controllers or of agreements between the latter and the beneficiaries of exceptions, or following the enforcement of administrative or jurisdictional authority orders;

(h) unlawfully removes or alters the electronic information referred to in Article 102¬d, or distributes, imports for distribution, broadcasts by radio or television, communicates or makes available to the public works or other protected subject-matter from which such electronic information has been removed or altered.

(h-bis) unlawfully, even in the manner set out in paragraph 1 of Article 85-bis of the Consolidated Law on Public Security, referred to in Royal Decree No. 773 of 18 June 1931, performs the fixation on digital, audio, video or audiovisual media, in whole or in part, of a cinematographic, audiovisual or editorial work or performs the reproduction, performance

or communication to the public of the fixation unlawfully performed.

Or whoever:

(a) unlawfully reproduces, duplicates, transmits or broadcasts, sells or otherwise places on the market, disposes of for any reason or unlawfully imports more than fifty copies or specimens of works protected by copyright and related rights

(a-bis) in violation of Article 16, for the purpose of gain, communicates to the public by placing it in a system of telematic networks, through connections of any kind, a work protected by copyright, or part of it

(b) by exercising in an entrepreneurial form activity of reproduction, distribution, sale or marketing, importation of works protected by copyright and related rights, is guilty of the acts referred to above

(c) promotes or organises the illegal activities referred to above.

- **Fraudulent production, sale, import, promotion, installation, modification, use for public and private use of apparatus or parts of apparatus suitable for decoding audiovisual transmissions with conditional access made over the air, by satellite, by cable, in both analogue and digital form (Article 171-octies of Law No. 633 /1941)**: anyone who, for fraudulent purposes, produces, offers for sale, imports, promotes, installs, modifies, uses for public and private use apparatus or parts of apparatus suitable for decoding audiovisual transmissions with conditional access made over the air, via satellite, via cable, in both analogue and digital form, shall be liable for this offence. Conditional access means all audiovisual signals broadcast by Italian or foreign broadcasters in such a form as to make them visible exclusively to closed groups of users selected by the party broadcasting the signal, irrespective of the imposition of a fee for the use of such service.

1.2. General rules of conduct

Employees of the Branch involved in the management of Risky activities are required, in order to prevent and prevent the occurrence of the types of crime in question, compliance with the following general principles of conduct:

- refrain from engaging in conduct, including associative behavior, such as to integrate the types of crime considered above (art. 25-novies of the Decree);
- refrain from engaging in or adopting behaviors and / or acts, including associative ones, prodromal to the subsequent realization of the types of offences indicated in this Section.

The Branch strictly prohibits its employees from reproducing, duplicating, disseminating, transmitting, marketing, by any procedure, without having the right and therefore abusively and for profit, a protected intellectual property, computer programs or content of databases on non-registered trademarks media.

In any way, the risky activities must be carried out in compliance with the laws in force, the rules

contained in the Code of Conduct, Code of Ethics and in this Model, expression of the values and policies of the Branch.

In particular, it is forbidden to acquire and use IT tools without a user license; it is also obliged to:

- verify the commercial and professional reliability of the suppliers of the branch;
- operate in compliance with the law and current internal regulations on the protection of copyright and industrial property.

Only the Financial Accounting & IT Department can make copies of software, for back-up or security purposes. All employees must ensure that no unlawful copies are made or used on the branch's premises.

The Branch provides that the employee during the Branch's Internet access shall not make or use illegal copies of copyrighted material, store such copies on the branch's equipment, or transmit these copies over the Branch network.

The risk of crime envisaged by art. 25-novies is controlled by procedural and application limitations and by continuous internal controls and monitoring as well as by rules and ethical principles of behavior.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Crimes involving breach of copyright is generally higher concern the following:

1. Data and Information Systems Management
2. Procurement of goods and services and appointment of professional assignments
3. Customer relationships
4. Management of gifts

1.3.1 Data and Information Systems Management

This Risk Activity concerns processes related to:

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;
b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Abuses concerning software and databases (Article 171-bis of Law no. 633/1941)

By way of example, this offence could be committed if the Branch, in order to obtain an unlawful advantage, understood as a profit deriving from the saving of economic resources, could, abusively, duplicate computer programs (such as, for example, software, etc.), avoiding purchasing the original ones protected by copyright.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Guidelines on System and Network Management
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Rules of IT General Management
- ICBC (Europe) S.A. Milan Branch IT System Manual
- Rules of Key Resources Security Management
- Security Management-Network&System Security
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC Privacy policy
- Information Security Policy
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- IT Governance-Equipment Management
- Measures of Information and Information System Security Management
- Rules of IT Resource Management
- Technical Specifications for Security Technique for Network System
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Abuses concerning software and databases (Article 171-bis of Law no. 633/1941)

By way of example, the offence could occur if the Branch purchases software products, databases and other intellectual works in violation of copyright law.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Centralized Procurement Rules
- Operating Expense Management Rules
- Financial Crime Policy
- Policy on the Management of the External Legal Advisors
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.3 Customer relationships

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Abuses concerning software and databases (Article 171-bis of Law no. 633/1941)

By way of example, the offence in question could occur if the Branch grants financing or provides services to persons involved in the illegal activities in question in order to facilitate them in carrying them out.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Credit Manual
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Banking Business Manual
- CIB Business Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Complaint handling Procedure
- Anti-Internal Fraud Policy
- PEP Procedure
- Customer Due Diligence Archiving Procedure
- BRAINS Manual

- DAC-6 procedure
- CRS procedure
- FATCA Procedure
- AML & Compliance Committee Charter
- Tax Affair Management Procedure
- Operating Expense Management Rules
- Third-party Management Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Measures Staff Recruitment
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.4 Management of gifts

This Risk Activity mainly concerns processes related to:

a) management of liberal initiatives;
b) management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Abuses concerning software and databases (Article 171-bis of Law no. 633/1941)

By way of example, the offence could arise if the Branch, in order to obtain an undue advantage, makes gifts to recipients that infringe copyright law.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy

- Centralized Procurement Rules
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. installation of software in compliance with acquired licences;
2. measures prohibiting the sale, copying, distribution of information, software and other forms of intellectual property in violation of licence agreements;
3. clear identification of the persons in charge of data management and information systems;
4. monitoring the effectiveness and operation of the IT security management system;
5. use of multi-layered firewalls to ensure the security of the Branch's website and IT system;
6. tracking of all IT events, problems and changes to the Branch's IT system;
7. verification and recording of gifts received in the "Gift Tracking Table;
8. clear identification of the people/departments in charge of the purchase of goods and services and the awarding of professional assignments;
9. accurate verification of the necessary qualifications, skills and requirements of suppliers
10. archiving of documentation relating to contracts with suppliers;
11. traceability in paper and/or electronic form of the conditions stipulated with customers;
12. periodical monitoring/control activities on the operations of the Branch also by the Surveillance Body;
13. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
14. staff awareness activities in the areas of the Branch's operations.

THIRTEENTH SECTION - INDUCEMENT NOT TO MAKE OR TO MAKE FALSE STATEMENTS TO JUDICIAL AUTHORITIES

1.1 Introduction

Article 25-decies of the Decree provides for the Entity’s administrative liability when an employee, pursuant to Article 377-bis of the Criminal Code, uses violence or threats, or offers or promises money or other benefit to induce not to make statements, or to make false statements any person who is called before the judicial authorities to make statements that can be used in criminal proceedings, if such person has the right to remain silent.

Moreover, pursuant to Article 10 of Law no. 146/2006 it can entail the same liability also where the offence is of transnational scope.

1.2 General rules of conduct

Employees of the Branch involved in the management of Risky activities are required, in order to prevent the occurrence of the types of crime in question, compliance with the following general principles of conduct:

- refrain from engaging in conduct, including associative behavior, such as to integrate the type of crime considered above (art. 25-decies of the Decree);
- refrain from engaging in or adopting behaviors and / or acts, including associative ones, prodromal to the subsequent realization of the types of offences indicated in this Section.

In any way, the risky activities must be carried out in compliance with the laws in force, the rules contained in the Code of Conduct, Code of Ethics and in this Model, expression of the values and policies of the Branch.

The Branch undertakes to ensure the autonomy of thinking of people who are required, or willing, to make statements before the Authorities, to refrain from interfering with such subjects in any way, including through violence, threats, offers or the promise of money or other benefits to induce not to make statements or to make false statements, so that the authenticity of the elements assumed by the Authorities are guaranteed.

In particular, the Branch guarantees the maximum collaboration with the judicial authorities and invites its employees to guarantee transparency during the investigations.

1.3 Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with offences of incitement not to make statements or to make false statements to the judicial authorities is generally higher concern the following:

1. Management of litigation and out-of-court procedures
2. Banking Supervisory Authorities relationship
3. Public Administration relationship
4. Staff selection, recruitment and management
5. Procurement of goods and services and appointment of professional assignments
6. Accounting
7. Management of payments
8. Data and Information Systems Management

1.3.1 Management of litigation and out-of-court procedures

This Risk Activity concerns processes related to:

a) complaints management;
b) management of active and passive judicial/out-of-court disputes (civil, criminal, administrative, labour law - debt collection) also with the external professional's assistance;
c) managing and monitoring settlement agreements.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, this offence could be configured when an employee of the Branch under oath (or in any declaration, certificate, verification, or statement) in any proceeding before or ancillary to any court knowingly makes any false material declaration or makes or uses any other information, including any book, paper, document, record, recording, or other material, knowing the same to contain any false material declaration or shall omit or destroy documentation in order to forbid the judicial lodge into the judicial proceeding.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Legal function working manual
- Policy on the Management of External Legal Advisors
- Complaint handling Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Anti Internal Fraud Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct

1.3.2 Banking Supervisory Authorities relationship

This Risk Activity concerns processes related to:

a) processing/transmission of occasional or periodic reports to the Supervisory Authorities;
b) requests/applications for licenses and/or authorisations;
c) feedback and compliance with applications/requests from the Supervisory Authorities;

d) management of relations with the Officials of the Supervisory Authorities during their inspection visits;
e) monitoring remediation actions and reporting/informing the Supervisory Authority.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, the offence could arise where the Branch offers or promises sums of money or other undue benefits, or intimidates by means of violence or threats, an employee so that he/she does not make statements or makes false statements to the judicial authorities, during inspections, inspections, audits in relation to facts concerning relations with the Supervisory Authorities.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Procedure for management of external inspections
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- AUI and SARA reporting procedure
- CRS procedure
- FATCA procedure
- Suspicious transaction reporting procedure
- AnaCredit Reporting Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct

1.3.3 Public Administration relationship

This Risk Activity concerns processes related to:

a) management of relations with Chambers of Commerce;
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding hygiene and safety and/or authorisations, permits, concessions;

d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;
e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office ;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police, Guardia di Finanza);
h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g. INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, the offence could occur where the Branch offers or promises sums of money or other undue benefits, or intimidates by means of violence or threats, an employee so that the latter does not make statements or makes false statements to the judicial authorities, during inspections, inspections, audits in relation to facts concerning relations with the Public Administration.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Anti-Bribery and Corruption Policy
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Gifts and Entertainment Policy
- Training Policy
- Code of Ethics
- Code of Conduct

1.3.4 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, the offence could arise where the Processor of the General Administration Department pays higher salaries than those due as a benefit to an employee in order to persuade him not to make statements, or to make false statements to the judicial authorities to the benefit of the Branch.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Measures Staff Recruitment
- Rights and duties of the employees' disciplinary measures
- HR Management System Instructions March 2023
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Employer Personal Data Processing Policy

- Operating Expense Management Rules
- Performance Appraisal Guidelines
- Training Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Internal Fraud Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.5 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, the offence could occur where the Branch pays a fee for services not received or for an amount higher than that due as a benefit to external suppliers/consultants/professionals, in order to induce them not to make statements or to make false statements to the judicial authorities.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Centralized Procurement Rules
- General Governance Policy of ICBC Milan Branch

- Policy on the Management of the External Legal Advisors
- Operating Expense Management Rules
- Financial Crime Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct

1.3.6 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;
c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;
f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Headquarter.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, this offence could occur if the Branch offers sums of money or other benefits not due, or intimidates by means of violence or threats, an employee, so that the same employee does not make statements or makes false statements to the judicial authorities, during inspections, inspections, checks on the keeping of accounting records.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Accounting Manual
- Anti Internal Fraud Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct

1.3.7 Management of payments

This Risk Activity concerns processes related to the management of the payment of sales/goods/services actually rendered/received.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, the offence in question could occur where the Branch pays its suppliers consideration for goods not received or for a higher amount than that due in order to induce them not to make statements or to make false statements to the judicial authorities.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Banking Business Manual
- Financial Affairs and Centralized Procurement Management Committee
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Anti-Internal Fraud Policy
- Centralized Procurement Rules
- Gifts and Entertainment Policy
- Whistleblowing Policy
- Conflict of interest Policy

- Third-party Management Procedure
- Code of Ethics
- Code of Conduct

1.3.8 Data and Information Systems Management

This Risk Activity concerns processes related to**:**

a) management of access and authentication/authorisation profiles to IT equipment, network and systems;
b) management of physical and logical perimeter security and equipment protection;
c) information and data security management;
d) computer Security Incident Management;
e) management of the copying and release within the company's information systems of computer programmes and application software without payment of the relevant rights and/or third-party licences;
f) development, implementation and maintenance of software, equipment, devices, connections, networks or technical components connected to the information system.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Inducement not to make or to make false statements to judicial authorities (Article 377-bis of the Criminal Code)

By way of example, this offence could occur where the Branch offers sums of money or other undue benefits, or intimidates by means of violence or threats, to an employee, so that he/she does not make statements or makes false statements to the judicial authorities, during inspections, inspections, investigations concerning the management of IT security incidents.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Guidelines on System and Network Management
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Rules of IT General Management
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure

- ICBC (Europe) S.A. Data Retention Policy
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- Technical Specifications for Security Technique for Network System
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- ICBC (Europe) S.A. Milan Branch Employer Personal Data Policy
- ICBC Privacy policy
- Information Security Policy
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- IT Governance-Equipment Management
- Measures of Information and Information System Security Management
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- Security Management-Network&System Security
- Whistleblowing Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of the persons/functions entrusted with the management of litigation and out-of-court procedures;
2. accurate verification of the necessary qualifications, skills and requirements of external lawyers;
3. clear identification of the persons in charge of interfacing with the Authorities;
4. traceability of communications/information between the Branch and the Judicial Authority;
5. implementation of all the actions of an organisational-accounting nature necessary to extract the data and information required by the Judicial Authority;
6. clarity and correctness of the Branch's financial and asset representation;
7. checks on the completeness, correctness and accuracy of the information transmitted to the Judicial Authorities;
8. archiving and preservation of documents;
9. filing and archiving of judicial documents;
10. periodic monitoring of the status of ongoing litigation, in coordination with the appointed external lawyers;

11. tracking, filing and storage of all documentation relating to the staff selection and recruitment process;
12. clear identification of subjects/functions for the appointment of professional assignments;
13. accurate verification of the necessary qualifications, skills and requirements of suppliers;
14. adequately formalised requests for tenders addressed to suppliers;
15. archiving of documentation relating to contracts with suppliers;
16. traceability of access and critical activities carried out through the company's IT systems
17. use of multi-level firewalls to ensure the security of the Branch's website and information system;
18. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
19. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
20. staff awareness activities in the areas of the Branch's operations.

As a further specification of the mitigation factors described above to protect against the risk of commission of the predicate offences referred to in Article 25-decies "Inducement not to make or to make false statements to Judicial Authorities", the following should be noted:

1. the Surveillance Body must be promptly informed of any request for information and/or news coming from the Judicial Authority, involving the Branch or the top management, from which it may be inferred that investigations or inspections are in progress;
2. it is not allowed to destroy or alter records, minutes, any kind of document (paper or electronic), or to make false statements to the Judicial Authority in anticipation of judicial proceedings, investigations or inspections;
3. external legal advisers must be formally selected and engaged by the Legal Department, subject to the approval of the General Management of the Branch;
4. in order to obtain high quality legal services, while ensuring an effective supervision and control of costs, the external legal advisors shall be selected only from the "ICBC Milan Branch Legal Panel List", prepared and updated from time to time by the Legal Function, also taking into account the proven capacities of the relevant law firms and specific agreements for legal fees;
5. in the event that the fee estimate provided by external lawyers exceeds the limit set by the Financial Affairs Committee, the Department making the request must obtain the approval of the Financial Affairs Committee in advance and prior to the appointment of the external counsel;
6. the work of external legal advisors is constantly monitored, the Legal Function examines what is produced by them and, if necessary, requests the appropriate amendments, additions or clarifications or any other necessary action;

7. when the assignment is completed and the invoice is submitted to the Legal Department, the latter must confirm the amount with the department head who requested the appointment of external lawyers. The invoice must be sent to the General Administration Department for a second check; the Head of the General Administration Department and the Head of the Financial Accounting Department must confirm the invoice, ensuring that the budget is in line with the request and the performance review has been completed. Once approved by the Head of the General Administration Department, the invoice must be submitted to General Management for final approval.

FOURTEENTH SECTION – OFFENCES AGAINST THE ENVIRONMENT

1.1. Introduction

This Section covers the offences envisaged by Article 25-undecies of the Decree, added by Legislative Decree 121/2011, i.e., the offences against the environment.

An offence against the environment is defined as any activity that damages the environment, which generally causes or may cause a significant deterioration of the quality of the air, including the stratosphere, soil, water, fauna and flora, including the preservation of species.

Specifically, the offences against the environment, set out in Article 25-undecies of the Decree, include:

- **Environmental pollution (Art. 452-bis of the Criminal Code)**: this offence is committed by anyone who unlawfully causes significant and measurable impairment or deterioration of water or air, or of large or significant portions of the soil or subsoil; of an ecosystem, biodiversity, including agricultural biodiversity, flora or fauna.
- **Environmental disaster (Art. 452-quater of the Criminal Code)**: anyone who unlawfully causes an environmental disaster is liable for this offence. An environmental disaster alternatively constitutes the irreversible alteration of the balance of an ecosystem; the alteration of the balance of an ecosystem whose elimination is particularly onerous and achievable only by means of exceptional measures; the offence against public safety by reason of the importance of the fact in terms of the extent of the impairment or of its damaging effects or by reason of the number of persons offended or exposed to danger.
- **Culpable offences against the environment (Article 452-quinquies of the Criminal Code)**: this offence shall be committed by any person who culpably commits the offences provided for in Arts. 452-bis and 452-quarter of the Criminal Code.
- **Trafficking in and abandonment of highly radioactive material (Art. 452-sexies of the Criminal Code)**: anyone who, unless the fact constitutes a more serious offence, unlawfully disposes of, purchases, receives, transports, imports, exports, procures for others, holds,

transfers, abandons or unlawfully disposes of highly radioactive material shall be liable for this offence.

- **Killing, destroying, capturing, taking, possessing specimens of protected wild animal or plant species (Art. 727-bis of the Criminal Code)**: anyone who, except where the fact constitutes a more serious offence, kills, captures, possesses, destroys, takes specimens belonging to a protected wild animal species, except where the action concerns a negligible quantity of such specimens and has a negligible impact on the conservation status of the species, shall be liable for this offence.
- **Destruction or deterioration of habitats within a protected site (Art. 733-bis of the Criminal Code)**: anyone who, outside the permitted cases, destroys a habitat within a protected site or in any case deteriorates it, thereby compromising its state of conservation, shall be liable for this offence.
- **Import, export, possession, use for profit, purchase, sale, display or possession for sale or commercial purposes of protected species (L. no. 150 /1992, Art. 1, Art. 2, Art. 3-bis and Art. 6)**: these provisions punish the import, export, transport, detention of animal or plant specimens in breach of Community and international provisions imposing special authorisations, licences and customs certifications, and in the falsification or alteration of the aforementioned documents and the detention of certain dangerous mammals and reptiles.
- **Discharges of industrial waste water containing dangerous substances; discharges to the soil, subsoil and groundwater; discharges into the sea by ships or aircraft (Legislative Decree No 152 /2006, Art. 137)**: this offence is committed by anyone who opens or, in any case, carries out new discharges of industrial waste water without authorisation, or continues to carry out or maintain such discharges after the authorisation has been suspended or revoked, as well as discharges of hazardous substances in excess of the limit values; or anyone who violates the prohibitions on discharges on the soil, into the subsoil and underground waters outside the cases allowed by Articles 103 and 104 of the Environment Code (C.A.) or into the sea by ships or aircraft.) or into the sea by ships or aircraft of dangerous substances envisaged by international conventions, except in the case of authorised discharges of rapidly biodegradable quantities, or whoever carries out the agronomic use of livestock effluents, of vegetation waters from oil mills, or of waste waters from farms and small agri-food companies, outside the cases and procedures envisaged therein, or does not comply with the prohibition or order to suspend the activity.
- **Unauthorised waste management activities (Legislative Decree no. 152 /2006, Art. 256)**: anyone who carries out waste collection, transport, recovery, disposal, trade and intermediation without the prescribed authorisation, registration or communication required by law, or the data controller of companies and the Processor of bodies that abandon or deposit waste in an uncontrolled manner or release it into surface or underground waters in

breach of the regulations in force, or anyone who creates or manages an unauthorised landfill or carries out unauthorised waste mixing activities or temporary storage at the place of production of hazardous medical waste in breach of the requirements laid down shall be liable for this offence.

- **Pollution of the soil, subsoil, surface water or groundwater (Legislative Decree No. 152/2006, Art. 257)**: anyone who causes the pollution of the soil, subsoil, surface water or groundwater by exceeding the risk threshold concentrations shall be liable for this offence, if he does not carry out remediation in accordance with the project approved by the competent authority within the framework of the procedure referred to in Articles 242 et seq.
- **Illegal trafficking in waste (Legislative Decree no. 152/2006, Art. 259)**: this offence is committed by anyone who ships waste constituting illegal trafficking within the meaning of Article 26 of Regulation (EEC) No 259/93 of 1 February 1993, or who ships waste listed in Annex II to said Regulation in breach of Article 1(3)(a), (b), (c) and (d) of said Regulation.
- **Violation of the obligations of communication, keeping of compulsory registers and forms (Legislative Decree No. 152/2006, Art. 258)**: persons liable for this offence who fail to make the communication prescribed by Article 189, paragraph 3, or make it in an incomplete or inaccurate manner or who fail to keep or keep in an incomplete manner the loading and unloading register or transport waste without the form referred to in Article 193 or indicate incomplete or inaccurate data on the form.
- **Organised activities for the illegal trafficking of waste (Art. 452-quaterdecies of the Criminal Code)**: anyone who, in order to obtain an unjust profit, with several operations and through the preparation of means and continuous organised activities, sells, receives, transports, exports, imports or in any case illegally manages large quantities of waste is liable for this offence.
- **False information on the nature, composition and chemical/physical characteristics of waste in the preparation of a waste analysis certificate; entering a false waste analysis certificate in SISTRI; omission or fraudulent alteration of the hard copy of the SISTRI form - handling area when transporting waste (Legislative Decree no. 152 /2006, Art. 260-bis)**: Producers of waste and other persons involved in its management (dealers, brokers, recovery or recycling consortia, persons carrying out recovery or disposal operations, transporters) who provide false information on the nature and characteristics of waste for the purpose of preparing a waste analysis certificate to be entered into SISTRI (waste traceability computer control system) or enter a false certificate into the system or use such a certificate to transport waste, or the transporter who accompanies the transport with a fraudulently altered paper copy of the SISTRI form filled in for the handling of waste.
- **Intentional/intentional pollution caused by ships (Legislative Decree no. 202/2007, Articles 8-9)**: this offence is committed by the Master of a ship, flying any flag, as well as the

crew members, the owner and the operator of the ship, if the infringement has occurred with their complicity, unless the act constitutes a more serious offence, who intentionally/intentionally pour into the sea polluting substances as referred to in Article 2, paragraph 1, letter b) or cause such substances to be spilled.

- **Cessation and reduction of the use of harmful substances (Law no. 549/1993 Art. 3)**: this provision prohibits the trade, use, import, export, and possession of atmospheric ozone-depleting substances listed therein.

1.2. General rules of conduct

Risk Activities must be carried out in compliance with applicable laws, the rules set forth in this Model and, also but not limited to, the provisions of the Code of Ethics and the Code of Conduct, an expression of the values and policies of the Branch.

Actions, operations carried out on behalf of the Branch must be guided by the principles of:

- separation of roles and responsibilities within the Branch;
- fairness, completeness and transparency of information;
- formal and substantive legitimacy;

in accordance with current regulations and according to established procedures.

Branch employees involved in the management of Risk Activities are required, in order to prevent the occurrence of the offenses in question, to comply with the following general principles of conduct:

- to abstain from engaging in conduct such as to integrate the types of offenses considered above (Article 25-undecies of the Decree);
- to abstain from engaging in or adopting behaviors and/or acts that are prodromal to the subsequent realization of the types of offenses indicated in this Section.

The Branch pursues the responsibility for the protection of the environment and provide finance to support sustainable activities as defined by EU taxonomy and Headquarter, reduce vulnerability arising from effects of climate change, the degradation of ecosystems, the loss of biodiversity, the risks associated with low social inclusion and a rise in equality.

1.3 Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Offences against the environment is generally higher concern the following:

1. Waste production, discharges, air emissions and soil pollution

2. Procurement of goods and services and appointment of professional assignments
3. Customer relationships
4. Credit-related activities
5. Managing relations with Business Partners and Financial Intermediaries

1.3.1 Waste production, discharges, air emissions and soil pollution

This Risk Activity concerns processes related to:

a) waste identification and classification process;
b) collection and management of temporary storage of waste;
c) purchasing and supplier management;
d) facilities management (air conditioning, water discharges, etc.);
e) management of cleaning services.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Environmental pollution (Article 452-bis of the Criminal Code)
- Culpable offences against the environment (Article 452-quinquies of the Criminal Code)
- Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006)
- Illegal trafficking in waste (Article 259 of Legislative Decree no. 152/2006)

By way of example, this in question could occur where the Branch carries out waste collection, transport, recovery, disposal, trading and intermediation activities in the absence of the authorisations, registrations or communications required by Legislative Decree no. 152/2006.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- ESG strategy action plan
- Third Party Management Procedure
- Code of Ethics
- Code of Conduct
- Staff handbook
- Sustainable Finance Policy

1.3.2 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Environmental pollution (Article 452-bis of the Criminal Code)
- Culpable offences against the environment (Article 452-quinquies of the Criminal Code)
- Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006)
- Illegal trafficking in waste (Article 259 of Legislative Decree no. 152/2006)

By way of example, the offence could occur if the Branch entrusts the disposal of plant and machinery to a company that is not duly authorised to transport and dispose of waste.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Operating Expense Management Rules
- General Governance Policy of ICBC Milan Branch
- Conflict of interest Policy
- Whistleblowing Policy
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct

1.3.3 Customer relationships

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Environmental pollution (Article 452-bis of the Criminal Code)
- Culpable offences against the environment (Article 452-quinquies of the Criminal Code)
- Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006)
- Illegal trafficking in waste (Article 259 of Legislative Decree no. 152/2006)
- Organised activities for the illegal trafficking of waste (Art. 452-quaterdecies of the Criminal Code)

By way of example, this offence could occur if the Branch, in conspiracy with a client in the unauthorised handling of large quantities of waste, fails to carry out checks on the references in its possession when establishing the contractual relationship.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Credit Manual
- Banking Business Manual
- Customer Due Diligence Archiving Procedure
- Financial Crime Policy
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Anti-Internal Fraud Policy
- CIB Business Manual

- BRAINS Manual
- Conflict of interest Policy
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct

1.3.4 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;
c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Environmental pollution (Article 452-bis of the Criminal Code)
- Culpable offences against the environment (Article 452-quinquies of the Criminal Code)
- Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006)
- Illegal trafficking in waste (Article 259 of Legislative Decree no. 152/2006)
- Organised activities for the illegal trafficking of waste (Art. 452-quaterdecies of the Criminal Code)

By way of example, this offence could be committed if the Branch gives a loan to a customer in order to provide support for illegal waste trafficking.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Credit Manual
- Financial Crime Policy
- AML-CTF Due Diligence and Client Onboarding Procedure
- Anti Internal Fraud Policy
- Banking Business Manual
- Charter of Credit Committee

- CIB Business Manual
- Conflict of interest Policy
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Whistleblowing Policy
- Gifts and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Code of Conduct
- Code of Ethics

1.3.5 Managing relations with Business Partners and Financial Intermediaries

This Risk Activity concerns processes related to:

a) identification and selection of business partners;
b) monitoring the situation of similar local banks;
c) preparation, organisation and execution of the marketing plan.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Environmental pollution (Article 452-bis of the Criminal Code)
- Culpable offences against the environment (Article 452-quinquies of the Criminal Code)
- Unauthorised waste management activities (Article 256 of Legislative Decree No. 152/2006)
- Illegal trafficking in waste (Article 259 of Legislative Decree no. 152/2006)

By way of example, this crime could occur if the Branch, in conjunction with selected business partners, abusively handles large quantities of waste through continuous organized activities.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Operating Expense Management Rules
- General Governance Policy of ICBC Milan Branch Internal Operation and Management Authorization
- Anti Internal Fraud Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Anti-Bribery and Corruption Policy

- Code of Ethics
- Code of Conduct

1.3. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. formal identification of persons charged with environmental roles and responsibilities regarding ESG;
2. implementation of an ESG Strategy Action Plan;
3. clear identification of the people/departments in charge of managing customer relations;
4. identification of customers;
5. periodic updating of information regarding customer relations in order to allow constant assessment of the customer's activity profile;
6. transparent and reconstructible decision-making processes over time related to credit assessment and terms and conditions stipulated with customers;
7. clear identification of the people/departments in charge of the purchase of goods and services and the awarding of professional assignments;
8. adequately formalised requests for tenders;
9. accurate verification of necessary qualifications, skills and requirements of suppliers;
10. archiving of documentation related to contracts with suppliers;
11. clear identification of the persons in charge of managing relations with business partners and financial intermediaries;
12. prior verification/due diligence in the selection phase of business partners/financial intermediaries;
13. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
14. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
15. staff awareness activities on environmental issues with actions oriented to continuous improvement.

FIFTEENTH SECTION - CRIMES OF EMPLOYMENT OF THIRD-COUNTRY CITIZENS WHOSE STAY IS IRREGULAR

1.1 Introduction

Article 25-duodecies of the Decree refers Article 22, paragraph 12-bis, Legislative Decree no. 286/1998 – Consolidated Law on Immigration which punishes employers that hire or make use of non-EU employees without a regular residence permit, or with a permit that has expired without requesting renewal or has been revoked or cancelled.

Specifically, Crimes of employment of third-country citizens whose stay is irregular, set out in Article 25-duodecies of the Decree, include:

- **Provisions against illegal immigration (Art. 12, paragraphs 3, 3-bis, 3-ter and paragraph 5, Legislative Decree No. 286/1998)**: anyone who, unless the fact constitutes a more serious crime, in violation of the provisions of the Consolidated Act on Immigration, promotes, directs, organizes, finances or carries out the transportation of foreigners into the territory of the State or performs other acts aimed at illegally procuring their entry into the territory of the State, or of another State of which the person is not a citizen or does not have permanent residence title, is liable for this crime in the case where:
    a) the act relates to the illegal entry or stay in the territory of the State of five or more persons;
    b) the transported person has been exposed to danger to his life or safety in order to procure his illegal entry or stay;
    c) the transported person was subjected to inhuman or degrading treatment to procure his or her illegal entry or stay;
    d) the act is committed by three or more persons in complicity with each other or by using international transportation services or documents that are forged or altered or otherwise illegally obtained;
    e) the perpetrators have the availability of weapons or explosive materials.

  Also liable for this crime is anyone who, in order to gain an unfair profit from the illegal condition of the foreigner or within the scope of the activities punished under this article, favors the permanence of the foreigner in the territory of the State in violation of the rules of the Consolidated Act on Immigration, unless the act constitutes a more serious crime.
- **Employment of illegal aliens (Art. 22, paragraph 12 bis, Legislative Decree No. 286/1998)**: the employer who employs foreign workers without a residence permit or whose permit has expired and whose renewal has not been applied for, within the terms of the law, or has been revoked or annulled, is liable for this offense.

1.2 General rules of conduct

Employees of the Branch involved in the management of Risky activities are required, in order to prevent the occurrence of the types of crime in question, compliance with the following general principles of conduct:

- refrain from engaging in conduct, including associative behavior, such as to integrate the type of crime considered above (art. 25-duodecies of the Decree);
- refrain from engaging in or adopting behaviors and / or acts, including associative ones, prodromal to the subsequent realization of the types of offences indicated in this Section.

In any way, the risky activities must be carried out in compliance with the laws in force, the rules contained in the Code of Conduct, Code of Ethics and in this Model, expression of the values and policies of the Branch.

In particular, the Branch has predisposed a specific selection process and hiring of staff. The Branch recruits staff from countries all over the world, both internationally and locally.

As part of the staff selection and recruitment process, the Branch also undertakes to hire staff that, if non-EU, has a valid residence permit throughout the period of employment.

1.3 Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Crimes of employment of third-country citizens whose stay is irregular is generally higher concern the following:

1. Staff selection, recruitment and management
2. Procurement of goods and services and appointment of professional assignments

1.3.1 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Employment of illegal aliens (Article 22, paragraph 12-bis, Legislative Decree no. 286/1998)

By way of example, he crime could take place in the case in which the Branch should hire foreign workers without a valid residence permit, or whose permit has expired and has not been requested, in accordance with the law.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Measures Staff Recruitment
- HR Management System Instructions March 2023
- Employer Personal Data Processing Policy
- Rights and duties of the employees' disciplinary measures
- Performance Appraisal Guidelines
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti Internal Fraud Policy
- Operating Expense Management Rules
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Third-party Management Procedure
- Training Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.2 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Employment of illegal aliens (Article 22, paragraph 12-bis, Legislative Decree no. 286/1998)

By way of example, this offense could occur if the Branch, in order to gain services at advantageous prices, enters into contracts with outside suppliers/consultants/professionals who employ foreign workers without valid residence permits in order to obtain savings on personnel costs.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Centralized Procurement Rules
- Policy on the Management of the External Legal Advisors
- Operating Expense Management Rules
- Financial Crime Policy
- Internal Operation and Management Authorization
- Third-party Management Procedure
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Financial Affairs and Centralized Procurement Management Committee rules
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4 Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of individuals/functions in charge of personnel selection, recruitment and administration;
2. transparency of the process of staff recruitment and employment, motivated by actual business needs, based on non-arbitrary criteria and as objective as possible;
3. verification of personnel's possession of valid residence permits;
4. traceability, storage and preservation of all documentation related to the personnel selection and hiring process;
5. adoption of measures to ensure a respectful, professional and dignified working

environment where equal opportunities are guaranteed;

6. accurate verification of the necessary qualifications, skills and requirements of suppliers;
7. archiving of documentation of contracts with suppliers;
8. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
9. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
10. staff awareness activities in the areas of the Branch's operations.

SIXTEENTH SECTION - RACISM AND XENOPHOBIA

1.1. Introduction

Article 25-terdecies of the Decree provides for an administrative liability of the entity in the event of instigation, provocation or propaganda that promote discrimination, or racial, ethnic, national or religious violence based on the denial or trivialization of the Holocaust or other crimes of genocide, war, or against humanity.

The article refers to the provisions envisaged by the Article 604-bis, paragraph 3 “Propaganda and incitement to commit racial, ethnic and religious discrimination” of the Criminal Code pursuant to which, unless the act constitutes a more serious crime, a person who propagates ideas based on racial or ethnic superiority or hatred, or incites to commit or commits acts of discrimination on racial, ethnic, national or religious grounds shall be punished who, in any way, incites to commit or commits violence or acts of provocation to violence on racial, ethnic, national or religious grounds or who promotes, directs, assists or participates in organizations, associations, movements or groups that incite discrimination or violence for racial, ethnic, national or religious reasons.

1.2. General rules of conduct

The Branch believes that diversity in its staff is critical to its success as a global organization, therefore, the Branch seeks to recruit, develop and retain the most talented people from a diverse candidate pool. Advancement at the Branch is based on talent and performance. We are fully committed to equal employment opportunity and compliance with fair employment practices and nondiscrimination laws. Consequently, the branch will not tolerate any acts of unlawful discrimination at work, whatever their form. In addition, retaliation against individuals for raising claims of discrimination is prohibited.

The Branch will refrain from any unlawful discrimination in all aspects of employment including recruitment, promotion, opportunities from training, career development, pay and benefits, discipline and selection for redundancy.

Person and job specifications will be limited to those requirements that are necessary for the effective performance of the job.

Also during the internet uses the employee must never send messages that are abusive, sexist, racist, defamatory, or which may offend in any way.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with racism and xenophobia is generally higher concern the staff selection, recruitment and management.

1.3.1 Staff selection, recruitment and management

This Risk Activity concerns processes related to:

a) profiling of potential candidates;
b) assessment and selection of candidates;
c) drafting the economic offer;
d) staff planning, updating and recruitment process.
e) employee database management (master data, salary data);
f) staff administrative management (attendance, days off, overtime, etc.);
g) management of travel and expense reports;
h) processing and payment of salaries;
i) management of employee relationships;
j) preparing, approving and sending tax, welfare and contribution declarations;
k) managing payments made by company credit cards;
l) management of training to be provided for employees;
m) conflict of Interest Management and Internal Reporting;
n) management and use of non-cash payment instruments.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Racism and xenophobia (art. 604-Bis, paragraph 3 of the Criminal Code)

By way of example, these types of offence occur in the event in which the GM refuses to approve the employment of a new entity, who has already passed the selection process for racial, ethnic, national or religious reasons.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Code of Ethics

- Code of Conduct
- Measures Staff Recruitment
- Staff Handbook
- Employer Personal Data Processing Policy
- Rights and duties of the employees' disciplinary measures
- HR Management System Instructions March 2023
- Operating Expense Management Rules
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Gifts and Entertainment Policy
- Performance Appraisal Guidelines
- Training Policy
- Third-party Management Procedure
- Anti Internal Fraud Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of individuals/functions in charge of personnel selection, recruitment and administration;
2. transparency of the process of personnel recruitment and employment, motivated by actual business needs, based on non-arbitrary criteria and as objective as possible;
3. provision of fair and anti-discriminatory employment practices;
4. definition of criteria related to the preparation of the economic offer;
5. traceability, filing and storage of all documentation related to the personnel selection and recruitment process;
6. adoption of measures to ensure a respectful, professional and dignified working environment where equal opportunities are guaranteed;
7. abstention from all forms of discrimination in all aspects of employment, including recruitment, compensation and promotions;
8. periodic monitoring/control activities on the operations of the Branch including by the Surveillance Body;
9. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
10. staff awareness activities in the areas of the Branch's operations.

SEVENTEENTH SECTION - FRAUD IN SPORTING COMPETITIONS, ILLEGAL PRACTICE IN GAMBLING SECTOR AND THROUGH BANNED MEANS

1.1. Introduction

This Section covers the offenses set forth in Article 25-quaterdecies of the Decree.

Article 5 of Law No. 39 of May 3, 2019, inserted Article 25-quaterdecies into Legislative Decree No. 231/01, specifying the administrative sanctions against legal persons, companies and associations for precisely the crimes of "fraud in sports competitions, abusive exercise of gambling or betting and gambling exercised by means of prohibited devices."

This case refers to all possible intentional and irregular changes in the conduct or outcome of a sports competition in order to interfere in whole or in part with the unpredictable nature of the competition itself in order to obtain an undue personal advantage or in favor of third parties, and to the same undue advantages obtainable through the abusive exercise of gambling or betting and games of chance exercised by means of prohibited devices.

Specifically, the Fraud in sporting competitions, illegal practice in gambling sector and through banned means, set out in Article 25-quaterdecies of the Decree, include:

- **Fraud in sports competitions (Art. 1, Law No. 401/1989)**: anyone who offers or promises money or other utility or advantage to any of the participants in a sports competition organized by the federations recognized by the Italian National Olympic Committee (CONI), the Italian Union for the Increase of Horse Breeds (UNIRE) or other state-recognized sports bodies and their member associations, in order to achieve a result other than that resulting from the proper and fair conduct of the competition, or performs other fraudulent acts aimed at the same purpose, is liable for this offense. Also liable for this offense is the participant in the competition who accepts the money or other benefit or advantage, or accepts the promise thereof.
- **Unauthorized exercise of gambling or betting activities (Art. 4, L. No. 401/1989)**: anyone who abusively exercises the organization of lottery or betting or wagering contests that the law reserves to the State or other concessionary body; anyone who, however, organizes bets or wagering contests on sports activities managed by the Italian National Olympic Committee (CONI), organizations dependent on it or the Italian Union for the Increase of Horse Breeds (UNIRE) is liable for this crime; anyone who abusively exercises the organization of public betting on other competitions of persons or animals and games of skill: anyone who sells on the national territory, without authorization from the Autonomous Administration of State Monopolies, tickets for lotteries or similar events of fortune of foreign states, as well as to anyone who participates in such operations through the collection of reservation of bets and the accreditation of the relevant winnings and the promotion and advertising carried out by

any means of dissemination ; anyone who in any way gives publicity to their exercise or participates in contests, jousts, bets operated in the manner referred to above, outside the cases of complicity in one of the crimes provided for therein; anyone who, without a concession, authorization or license pursuant to Article 88 of the Consolidated Text of Public Security Laws, approved by Royal Decree June 18, 1931, no. 773, and subsequent amendments, carries out in Italy any organized activity for the purpose of accepting or collecting or in any way facilitating the acceptance or in any way the collection, including by telephone or telematic means, of bets of any kind by anyone accepted in Italy or abroad; anyone who carries out the collection or reservation of lotto bets, betting contests or wagers by telephone or telematic means, where he or she does not have the appropriate authorization to use such means for the aforementioned collection or reservation.

1.2. General rules of conduct

Risk Activities must be carried out in compliance with applicable laws, the rules set forth in this Model and, also but not limited to, the provisions of the Code of Ethics and the Code of Conduct, an expression of the values and policies of the Branch.

Branch employees involved in the management of Risk Activities are required, in order to prevent the occurrence of the offenses in question, to comply with the following general principles of conduct:

- to abstain from engaging in conduct such as to integrate the types of offenses considered above (Article 25-quaterdecies of the Decree);
- to abstain from engaging in or adopting behaviors and/or acts that are prodromal to the subsequent realization of the types of offenses indicated in this Section.

The risk of crime under Article 25-quaterdecies is mitigated by procedural and enforcement limitations and continuous internal controls and monitoring, as well as by internal rules and ethical principles of behavior.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with fraud in sporting competitions, illegal practice in gambling sector and through banned means is generally higher concern the management of gifts and sponsorships.

1.3.1 Management of gifts and sponsorships

This Risk Activity mainly concerns processes related to:

a) Management of liberal initiatives;
b) Management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraud in sports competitions (Article 1, Law No. 401/1989)

By way of example, this crime could occur if the Branch carries out sponsorship in favor of entities operating in the field of sports competitions and gambling management in order to contribute to the achievement of a result other than that resulting from the proper and fair conduct of the competition.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Gifts and Entertainment Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Centralized Procurement Rules
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of people/functions in charge of handling sponsorships, gifts or gratuities;
2. formal definition of the process for requesting, verifying and approving sponsorships, gifts or gratuities;
3. archiving of documentation related to sponsorships and gifts and gratuities;
4. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
5. suitable system for sanctioning non-compliance with the measures indicated in the Model;
6. staff awareness activities in the areas of the Branch's operations.

EIGHTEENTH SECTION - TAX PREDICATED OFFENSES

1.1. Introduction.

The rules implemented have the purpose of preventing and fighting the tax evasion at EU level including specific offences related to "income taxes" and "value added taxes" (VAT) as provided for and by the Legislative Decree No. 74/2000, and as extended by the so-called EU -"PIF Directive" (EU Directive 2017/1371), which enhanced its repression by including provisions of the European legislation in order to protect the interests and not to affect the public finance of the Union.

Tax-related offenses have been listed in Article 25-quinquiesdecies Legislative Decree 231/01.

The categories of Tax Predicated Offenses, on a general basis, are:

(A) "Declarative" crimes (the attempt pursuant to Article 6 of Legislative Decree No. 74/2000 is also punished, including all preparatory acts in order to draft the fraudulent declaration, also consisting in writing untrue information in accounting; it is constituted even if the facts take place partly in Italy and the rest of offence in other State - Headquarter - EU.)

(B) Crimes of "omission" (not making declarations or payments legally binding and due).

(C) Any other "facilitating conduct" constituting the offense under (A) and under (B) above, even when implemented in the context of the customer's relationships or in the transactional operations with customers.

Specifically, the Tax Predicated Offenses set out in Article 25-quinquiesdecies of the Decree include:

- **Fraudulent declaration through the use of invoices or other documents for non-existent operations** ((art. 2 Legislative Decree no. 74/2000): the offense is committed by anyone who submits declarations relating to income taxes or VAT that indicate fictitious passive elements, resulting from invoices or other documents recorded and stored in the accounting records considered mandatory by law or kept for tax purposes (and related proofs). The invoices or documents used are characterized by material or ideological falsehood about the existence, in whole or in part, of the transactions indicated therein, or about the counterpart subject.

  Example: invoices are issued for services that have never been performed or have been performed to a third unrelated party and fictitious passive elements are inserted among the accounting elements, thus obtaining fraudulent savings.
- **Fraudulent declaration by other means ((Article 3 of Legislative Decree no. 74/2000):** the offense exists when, apart from the case of use of invoices or documents certifying non-

existent transactions as above and before mentioned, in one of the aforementioned declarations are indicated active elements lower than the actual ones, or are exposed fictitious passive elements, concerning credits and withholdings too, even though the signing of simulated transactions, both objectively or subjectively, or by the means of using false documents, recorded in the obligatory accounting records or kept for proof purposes, or any other fraudulent means sufficient and/or able in falsifying the accounting by hindering the assessment or creating declarative effect to mislead the Revenue Agency.

The crime is committed if both: (a) tax evaded exceed 30,000.00 Euro; b) the overall amount of the assets, even through the use of not real costs, exceed 5% of the overall declared amount or exceed 1,500,000.00 Euro or the overall credits and the false costs deducted by the payable taxes exceed the 5% of the same payable amount or, in any case, the amount is equal or exceed the amount of 30,000.00 Euro

This offense doesn't exist/is not committed if and when certain thresholds are not exceeded, or the false representation of reality is not obtained by artifice, but it is a mere omission of invoice and annotation/registration/storage obligations or only indicating in the declaration active elements lower than the real ones.

Example: the offense is committed using false documentation/invoices in order to evade income tax, thus obtaining fraudulent savings for the Branch or it can also be completed when the false documents are held as evidence against the Tax Authority. It can be configured, by way of example, in using invoices for services never performed by calculating the paid fees/costs in the VAT return.

- **Unfaithful declaration (Article 4 of Legislative Decree no. 74/2000):** these offenses are sanctioned in case of obtaining fraudulent savings and:
  - in the annual income tax or VAT returns are indicated/declared active elements for an amount lower than the current one or non-existent passive elements;
  - does not submit to reporting, being obliged to do so, one of the declarations relating to said taxes (or the withholding tax declaration).

  However, such conduct(s) entail administrative responsibility pursuant to Legislative Decree no. 231/2001 only if they relate to the evasion of VAT for an amount not less than 10% of the active elements indicated or is, in any case, greater than € 2 million and if they are committed in the context of cross-border fraudulent systems.

  Example: this is the conduct that consists in indicating in the declaration's assets for an amount lower than the actual amount or non-existent liabilities, to evade income or VAT tax, thus obtaining fraudulent savings for the company.
- **Omitted declaration (Article 5 of Legislative Decree No. 74/2000):** this offense is sanctioning anyone who does not submit to the TAX Authority the tax declaration (return or VAT declaration) and the tax evasion exceed the amount as of 50,000.00 Euro per each

single tax obligation.

Example: the tax declaration is classified as omitted if it has not been submitted to the Tax Authority within No. 90 days by the due date.

- **Undue compensation (Article 10-quater of Legislative Decree No. 74/2000):** this offense is sanctioning anyone who:

  • does not pay taxes that are due using unpaid credits as compensation, for an annual amount exceeding a certain threshold (for each single tax 50,000.00).

  Example: the Branch fails to make payments due for the tax year, offsetting taxes and contributions through the use of VAT receivables not due for an amount exceeding € 50,000.00. The crime is committed by making both an omissive conduct and by using an undue compensation between debit and credit amounts payable to the tax Authority so qualifying the crime.

- **Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000):** the crime is committed by anyone who issues to third parties' invoices, in cooperation with third parties, and requires to deduct from taxes invoices or any other documents for non-existent transactions in order to evade income taxes or VAT. The crime is committed irrespective of the amount of invoice.

  Example: the offense is committed by whoever issues invoices for non-existent transactions, in order to allow a third party to evade income or value added taxes (VAT).

- **Hiding or destroying account documents (Article 10 of Legislative Decree no. 74/2000):** the crime is committed by whoever, in order to evade income taxes or VAT or to allow third parties to evade them, conceals or destroys all or part of the accounting records or documents which must be stored, in order to prevent the reconstruction of income or turnover. The crime is committed irrespective of any amount.

  Example: this crime involves the destruction, even partial, of the obligatory accounting records with the impossibility of reconstructing the transactions for tax purposes.

- **Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000):** the sanctioned conduct consists in doing any act and/or performing any transaction by selling assets diverting sums to evade the payment of taxes that are calculated and required as due. It's committed on assets by any conduct and/or by making any simulated act and/or fraudulent dispositive acts, consistent in making ineffective/incapable any request and/or compulsory and executive procedure by the Tax Authorities.

  The conduct is related to those who, in the context of a tax transaction procedure, in order to obtain for themselves or others a lower payment of taxes and accessories, indicate in the documentation of the official declaration assets lower than real or fictitious passive elements for a total amount exceeding Euro 50,000.

  Example: an executive with the powers disperses and / or alienates the company's assets in

order to evade the payment of taxes, obtaining a fraudulent tax saving for the Branch.

The commission of such offenses involves the administrative liability of the Entity pursuant to Legislative Decree no. 231/2001 and pertains to both (A) “declarative” facts or events and also (B) “omissions” that involve the so-called "Active cycle" and the "passive cycle" of the accounting and tax obligations declarations as well as the archiving of documents, and again it is potentially configurable, also (C) in the context of relations with customers who commit conduct that configure the aforementioned crimes as conduct which consists in omitting to report or facilitate customers following the transactions carried out through the Branch.

1.2. General rules of conduct

All Recipients are required to act in compliance with current laws and best tax practice, in order to protect the Branch from any conduct that constitutes tax crimes also by means of structured declarations on altered accounting data and / or on non-existent documents and / or incorrect tax practices, even in aggregation with other data or conduct, or even omitting payments due or facilitating customer operations in conduct that constitute a tax crime.

The Branch carried out an internal risk analysis and internal wide evaluation concerning the activities of its departments and established the more wide and restrictive interpretation to be compliant with tax rules and as qualified as "tax compliance", whether understood as:

(a) direct compliance (carrying out the activities of the Branch);

or also

(b) indirect compliance (carrying out transactions on behalf of customers or proposing new products, services or banking and financial activities);

considering those as included in the General Government Policy, and the “Code of Conduct.” and the “Code of Ethics” of the Branch that all employees must strictly comply with, such as direct expression of the anti-tax evasion protocols. The violation, even partial, of the protocols established in the Model is qualified and constitutes a serious disciplinary offense.

Since the Tax Predicated Offenses can, at first level, be originated from false or very inaccurate declarations and / or from any omitted payment of amounts to be considered mandatory and due but also from the application of taxes (withholding tax) and also from the artificial evaluation (including transfer price evaluation) and / or instrumental transfer of significant assets and / or any conduct facilitating the completion of fiscally incorrect (material and severe effect) transactions by customers (including cross-border transactions), all declarations and settlement of taxes as well as activities that fall within the fulfilment of tax-related obligations, must be inspired and be compliant with the following principles:

- formal and substantive legality;
- managing and keeping the accounts in a clear and truthful manner;

- reliability and integrity of accounting and management information;
- preventive assessment of the tax effects of new banking products, activities or services (also in terms of potential improper or illegal use by customers) or in transactions carried out with customers in which the Branch is part of which the tax effects;
- making the payment of taxes, duties or contributions (even in the case of active repentance) on time;
- correct application of the rules on "transfer pricing";
- correct implementation and adoption of the IAS / IFRS principles and rules;
- correct classification of financial assets;
- correctness, completeness and transparency of data and information (especially for the Tax Authority; and for auditors);
- full tax compliance and constant compliance with current legislation and in reliance with the Tax Authority's established practices.

Regarding the legal and binding reporting communications to be made and reported to the Tax Authority, the data and information must be complete, truthful and correct and it is mandatory to promptly produce any document (also referring to customers) that is requested by the Tax Authority.

For all Recipients it is forbidden to:

- induce someone to expose or directly use into the tax declarations, or to input false and incorrect data in the accounting and management systems and in the registers of the Branch, or to use invoices or other non-existent accounting elements or make false assessments or omit or destroy accounting data and information, or make any other activity and/or conduct in order to make or lead to declarations false or incorrect or mislead the Tax Authority or obtain for the Branch or allow customers to obtain an illegal tax advantage;
- facilitate, in a broader and more general sense, any illegal conduct that may result in an illegal tax advantage, including customers' interests and illegal fiscal advantage;
- prevent or hinder the performance of control or audit activities legally attributed to the Tax Authority or the audit company, including through the destruction of documents.

The keeping of the accounts and the fulfilment of tax obligations, both declarative (in details income and VAT) and payment, is strictly based on the general principles of truth, accuracy, completeness, clarity and transparency of the recorded data and must be made always on time (in case of any diligent change too).

Each accounting element used for tax purposes must comply with current legislation and must be tracked and adequately documented and stored in compliance with the form and substance and compliance with the purpose as required by the regulations and procedures in force, in order to allow a complete reconstruction and legal proof.

The Branch undertakes to ensure the accuracy of the keeping of documents and tax records and to declare their full compliance with applicable laws in force so that all the declarations of the Branch and the settlement of taxes are always (and are reasoned to be) in compliance with tax laws, interpreted according to correct tax practice, constituting, under all relevant aspects, a true and correct representation. The assessment criteria are based on the provisions of tax law, interpretative practices and circulars and the responses to questions formulated by the Tax Authority, accordingly to the rules and criteria applicable to the credit sector.

Recipients are required to refrain from any conduct, active or omissive or by facilitating any illegal customer conduct that violates, directly or indirectly, the aforementioned principles or internal procedures relating to the acquiring and/or drafting of accounting documents and tax returns and liquidation to the Tax Authority.

In addition, anyone who has accounting duties and / or related to tax returns (in particular Financial Accounting Department) and/or is involved in the authorization of new products or services or must proceed with the sending of data requested by the Tax Authority (in particular Legal and Compliance Department) is required to keep up to date by carefully reading each internal circular or from the accounting and tax consultants, as well as participating in all the planned training initiatives, in order to better understand the conduct that constitutes tax offense. It is essential that the Recipients are able to know the operations that may be connected to tax laundering evasion practices in order to prevent them, as well as in a strict sense be compliant with the reporting obligations to the Tax Authorities aimed at the acquiring of any data and / or useful information to fight international tax evasion too.

The reporting includes:

(a) the adequate acquiring and store and update of all customer's and financial relationships falling within this scope of cooperation with the Tax Authority;
(b) the reporting of tax cooperation against tax evasion (DAC 6, FATCA and CRS - Common Reporting Standard -);
(c) any information or document requested by the Tax Authorities.

Each Recipient is required to report all cases in which there are reasonable grounds to believe that tax crimes are or may have been committed or that false or seriously incorrect accounting of data, evaluation in the financial statements and / or significant costs and / or use of invoices for non-existent transactions are ascertained. The conduct must be promptly reported by using the whistleblowing procedure.

In the said context, the Branch undertakes to:

- diligently and promptly carry out any tax obligation or tax declaration and any payment arising from legal obligations;
- correctly apply the rules on transfer pricing and the correct evaluation of financial assets;

- correctly apply the IAS / IFRS principles and rules;
- correctly apply the rules of the budget and financial plan;
- keep the accounting documents in order to avoid destruction or concealment;
- carry out a preventive analysis of tax impact for all new financial products, activities and / or services offered to customers, identifying and countering potential conduct (also by customers that involve the operations of the Branch) such as to complete tax offences;
- carry out, both internally and also with the help of external firms or professionals, any tax compliance verification activity, including updating the local practices and procedures adopted, including legal communications to the Tax Authority;
- operate in such a way as to avoid any implication in the structuring of operations or the completion of suitable transactions, even if only potentially, to favour aggressive and / or elusive tax conduct or practices and / or constitute a risk of use for tax evasion, for the effect , acting in full compliance with the tax legislation, from time to time, in force;
- check in advance, with diligence and with any professional and careful way, the relevant accounting information as available and also those acquired by or given by the suppliers and / or relevant documents, including those from customers, in order to assess their correctness and adequacy in order to maintain customer's relationships;
- include in the context of the whistleblowing procedure any and all unlawful tax conducts or cases in which there're reasonable grounds to believe that punishable offenses are or may have been committed in relation to false or seriously incorrect accounting of data, financial statement items and / or other costs and / or purchase and / or use of invoices for non-existent transactions.

1.3. Activities classifiable at risk pursuant to Legislative Decree 231/01 and the main methods of committing crimes.

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with Tax predicated offenses is generally higher concern the following:

1. Accounting
2. Customer relationships
3. Tax management
4. Procurement of goods and services and appointment of professional assignments
5. Public Administration relationship
6. Banking Supervisory Authorities relationship
7. Operational Cost Management
8. Management of gifts

9. Customer account management and monitoring
10. Credit-related activities

1.3.1 Accounting

This Risk Activity concerns processes related to:

a) management of the branch's financial budget;
b) management of accounting records;
c) management of supplier/customer master data;
d) management of all activities related to active/passive invoicing;
e) management of non-performing loan recovery activities and related loss forecasts;
f) keeping of accountancy records, preparation of financial statements, annual reports, corporate communications in general;
g) management of relations and assisting the external Auditor;
h) management of accounting reports required locally, by the Head Office and Headquarter.

Listed below are the types of crime that are abstractly applicable and the related methods of commission:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other devices (Article 3, Legislative Decree No. 74/2000)
- Issue of invoices for non-existent transactions (Article 8, Legislative Decree No. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Omitted declaration (Article 5, Legislative Decree 74/2000)
- Undue compensation (Article 10-quater, Legislative Decree 74/2000
- Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000)

By way of example, the commission of offenses can take place/be committed/ in the active and / or passive cycle of accounting and subsequently in the tax declarations in the event that:

(a) the receipt and / or issuance of invoices for non-existent transactions is accepted, required to customers and/or permitted (also by way of negotiation / conclusion of contracts relating to the purchase of goods and services, the execution of works and the assignment of consultancy services) and / or are inserted in the management systems so that data are reported or is made a data input (or modified) into the accounting that do not correspond to the truth (for example by inserting false suppliers or customers or in any case false cost amounts in the management and accounting system of the Branch);
(b) assessments and performing of tax declaration(s) are made, including data or other elements for tax returns (in particular income 770 or VAT IRES and IRAP - with the assistance of the external

firm) and in fulfilment of tax obligations (withholding tax; substitute tax and application tax virtual stamp duty) in a manner that's in breach of law or tax practice;

(c) omissions are made and / or false or altered data reported in the accounting and tax returns are implemented such as to be reported or induce to alter the correctness of the accounting and tax communications required by law towards the Tax Authorities;

(d) is omitted a full and adequate compliance with all the tax deadlines (income and VAT).

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Accounting Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Credit Manual
- Anti Internal Fraud Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Operating Expense Management Rules
- Anti-Bribery and Corruption Policy
- Third Party Management
- Code of Ethics
- Code of Conduct

1.3.2 Customer relationships

This Risk Activity concerns processes related to:

a) amending and/or updating client account information;
b) storage of correspondence between customers and the Branch;
c) monitoring of client credit risks;
d) analysing documents and checking references;
e) Conflict of Interest Management and Internal Reporting;
f) AML/CTF compliance management and customer onboarding procedure (Monitoring AML/CFT regulatory updates; Customer due diligence - or Enhanced Due Diligence-; Audits and checks on sensitive lists for AML/CFT purposes; SOS; Staff training; Relationships with PEP and/or high-risk customers);
g) Management of payments related to customers.

The Branch on an ordinary principle and basis evaluates in advance any fiscal impact on banking activities and products and has proceeded to analyse any potential "reportable transaction" and "illicit tax scheme" (as per DAC-6 too) in which the bank could be involved by customers operations;; in details, any cases involving potential tax crimes committed by customers can be effectively cracked down and the same are not, even indirectly, facilitated by products and / or services of the Branch and / or by conduct implemented by the Recipients in their favour.

As part of the activities carried out on behalf of customers, the Banking Department and the Financial Institutions Department are liable for the operations under their responsibility (including trade finance operations – import and export letters of credit – collections, T / T, import and export discounts, forfaiting, factoring, refinancing, export financing, advance financing, guarantees, etc.) which may imply on the customers' side the use of tax fraud mechanisms, including and not limited to avoiding payment of the Community VAT, and / or documents (even non-existent) and / or fictitious costs such as to constitute cases of criminally relevant tax evasion, especially when implemented in the context of ongoing relationships, through operations with the Branch.

Listed below are classified the types of crime that are abstractly applicable and the related methods of commission:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000).
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000).
- Unfaithful declaration (Article 4, Legislative Decree 74/2000).
- Undue compensation (Article 10quater, Legislative Decree 74/2000).

By way of example: this type of crime could occur when one is faced with (or are detected and easily detectable) operations that constitute operational mechanisms that fall and/or are included within the tax fraud scheme (also highlighted by the sector authorities as sectorial risks – for example the UIF -) and / or obvious abnormalities (assets underlying the trade finance transaction) and/or not proceeding by carrying out the necessary and/or mandatory checks (on high risk customers or the ones reported for suspicious transaction for fiscal anomalies too) pursuing an interest in maintaining the relationship with the customer.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Tax Affair Management Procedure
- FATCA Procedure
- Dac-6 procedure
- CRS procedure
- Banking Business Manual

- Credit Manual
- AML-CTF Due Diligence and Client Onboarding procedure
- Suspicious Transaction Reporting procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Anti Internal Fraud Policy
- Code of Ethics
- Code of Conduct

1.3.3 Tax management

This Risk Activity concerns processes related to:

a) drafting, approving and sending tax declarations or payment forms;
b) direct and indirect taxes payments;
c) management of active/passive invoicing;
d) storage of accounting records.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000)
- Hiding or destroying account documents (Article 10 of Legislative Decree no. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000)

By way of example, this crime could occur if the person in charge of preparing corporate accounting documents, conceals or destroys all or part of the accounting records or documents whose preservation is mandatory, so as not to allow the reconstruction of income or business volume in order to evade income tax or value added tax.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Tax Affairs Management Procedure

- CRS Procedure
- FATCA Procedure
- Dac-6 procedure
- Financial Accounting Manual
- Treasury Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Anti-Bribery and Corruption Policy
- Credit Manual
- Suspicious Transaction Reporting procedure
- Anti Internal Fraud Policy
- Code of Ethics
- Code of Conduct

1.3.4 Procurement of goods and services and appointment of professional assignments

This Risk Activity concerns processes related to:

a) classifying and monitoring suppliers/consultants/external professionals;
b) tracking and selection of external suppliers/consultants/professionals;
c) drafting and approval of cost authorisations;
d) contract / purchase order drafting and management;
e) acceptance of goods, works, services and professional advice and issuing of approval for payment;
f) use of Branch goods and services: activities related to the use of the Branch's assets and equipment (IT tools, information dissemination tools, text/video duplication devices, etc.);
g) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000)
- Omitted declaration (Article 5, Legislative Decree 74/2000)

- Undue compensation (Article 10-quater, Legislative Decree 74/2000
- Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000)

By way of example, the offense could occur if the Branch issues invoices for non-existent transactions related to the purchase of goods and services or the awarding of professional appointments and consequently enters them into accounting systems for the data to be reported.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Operating Expense Management Rules
- Financial Crime Policy
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Third-party Management Procedure
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Gifts and Entertainment Policy
- Code of Ethics
- Code of Conduct

1.3.5 Public Administration relationship

This Risk Activity concerns processes related to:

a) management of relations with Chambers of Commerce;
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding hygiene and safety and/or authorisations, permits, concessions;
d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;
e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office ;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police,

Guardia di Finanza);

h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g. INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

In the fiscal context, the Tax Authority has structured and implemented on a local basis and has a specific local requirement concerning a data exchange system used to carry out tax assessments and verification and has also joined international cooperation agreements aimed at exchanging data to effectively prevent tax evasion, including non-payment of VAT.

It is essential that the communications due for the applicable sector provisions on relationships (such as FATCA and CRS) and / or even those "upon event" on the completion of significant transactions - "reportable transactions" - (DAC 6) are always promptly identified, fulfilled and updated.

Activities performed by the Branch, as per DAC-6 analyses and from a fiscal point of view (that is also autonomous and additional to the protocols of the "Tenth Section" - Crimes of receiving stolen goods, money laundering and use of money, goods or utilities of illicit origin, as well as self-laundering, include -

- the identification activities at the time of establishing and maintaining the relationship with customers and the performing of cross-border activities;
- (in general/on a general basis) the fulfilment of the declaratory and reporting obligations related to both the provisions relating to Italy's participation in international agreements relating to the exchange of data and cooperation against international tax evasion;
- the definition and updating of the data relating to the tax database on which all the Tax Authorities, both national (Registry of Financial Relations) and international (especially CRS), carry out tax assessments aimed at combating elusive practices.
  Regarding reporting activities, also for the purposes of DAC6 (Directive of the European Council (EU) 2018/822 amending Directive 2011/16 / EU) - implemented by Legislative Decree no. 100/2020 -, reference is made to fiscal risk events (hallmarks for DAC-6) as well as customer’s transactions deriving from the risk analysis carried out on the activity of the Branch (type and transactions) and updated, time by time, according to the " offer of activities, products and / or services.
- Risk events that identify both activities of (I) a potential unlawful advantage of the Branch identifiable, at a potential level, as follows: (i.1) in credit and/or transactional and cross border activities (where there’s knowledge and/or detections or severe indications that the client may be looking for and/or is requiring or aiming to obtain an illicit tax advantage);

(i.2) in payment services and/or cross-border transactions (in case the Branch of omits the reporting obligations); (i.3) in the structure of relationships or operations (where there's knowledge or severe indications and material triggers that the customer may be seeking to obtain an illicit tax advantage); and also concerning (II) the omission - partial too or specific for some customers - of CRS reporting obligations, also with reference to the supplementary obligations that Headquarter have to carry out on a tax resident in Luxembourg;

- reporting of "reportable transactions" on DAC-6 tax risk events on an independent basis and irrespective of the anti-money laundering reporting obligation (Legislative Decree no. 231/07 art. 35) or to the Tax Authority.

  It is also important to monitor the consistency and coherence of the data sent to the Tax Authority with those acquired by the Customer for anti-money laundering purposes and kept available for the Authorities, including tax (Legislative Decree No. 231/07 art. 31 and ss.).

Here below described, in compliance with the premise, the types of crime abstractly applicable in the sense indicated above are listed:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Omitted declaration (Article 5, Legislative Decree 74/2000)

By way of example, the commission of crimes can take place/be committed both in the declarative and/or through the transactional context. It includes any conduct facilitating illegal tax evasion that can be committed by customers. It can be performed on a cooperative basis with the client by (i) facilitating customer's conducts through banking or financial products; (ii) omitting the reporting to the Tax Authority of customer's relationship as required by law (Central database of Financial Relationships); (iii) omitting the "reportable transactions" (DAC-6) that are eligible; (iv) making any other conduct allowing the tax evasion of the Customers (i.e. issuing invoices for non-existent operations and / or producing to customers accounting statements and/or tax costs that are known not to be true.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations

adopted by the Branch:

- Financial Crime Policy
- General Governance Policy of ICBC Milan Branch
- Anti-Bribery and Corruption Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Third-party Management Procedure
- Gifts and Entertainment Policy
- Training Policy
- Code of Ethics
- Code of Conduct

1.3.6 Banking Supervisory Authorities relationship

This Risk Activity concerns processes related to:

a) processing/transmission of occasional or periodic reports to the Supervisory Authorities;
b) requests/applications for licenses and/or authorisations;
c) feedback and compliance with applications/requests from the Supervisory Authorities;
d) management of relations with the Officials of the Supervisory Authorities during their inspection visits;
e) monitoring remediation actions and reporting/informing the Supervisory Authority.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Omitted declaration (Article 5, Legislative Decree 74/2000)

By way of example, the offense could occur if the Branch conceals or destroys accounting records during inspection visits by the Supervisory Authority.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- CRS procedure
- FATCA procedure
- Procedure for management of external inspections
- AUI and SARA reporting procedure
- Suspicious transaction reporting procedure
- AnaCredit Reporting Procedure
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Operating Expense Management Rules
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.7 Operational cost management

This Risk Activity mainly concerns processes related to the review and approval of daily operational costs.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000)
- Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Omitted declaration (Article 5, Legislative Decree 74/2000)

By way of example, this offense could occur if an offense is committed where the Branch issues invoices to third parties regarding non-existent transactions in order to evade income tax or VAT.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Financial Accounting Manual
- Operating Expense Management Rules
- Credit Manual
- Banking Business Manual
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Centralized Procurement Rules
- Financial Affairs and Centralized Procurement Management Committee rules
- Whistleblowing Policy
- Anti Internal Fraud Policy
- Gift and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.8 Management of gifts

This Risk Activity mainly concerns processes related to:

a) management of liberal initiatives;
b) management of processes relating to gifts, entertainment expenses, charities and sponsorships.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Omitted declaration (Article 5 of Legislative Decree No. 74/2000)
- Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000)

By way of example, this offense could occur if the Branch makes gifts to those who have provided it with support by carrying out simulated transactions in order to evade income tax or VAT.

The Recipients of the Model who operate in the context of this activity, in compliance with the general

principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Gifts and Entertainment Policy
- Anti-Bribery and Corruption Policy
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Whistleblowing Policy
- Conflict of interest Policy
- Third-party Management Procedure
- Centralized Procurement Rules
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.3.9 Customer account management and monitoring

This Risk Activity concerns processes related to:

a) customer account profile management
b) account opening/closing;
c) management of dormant customers, dormant accounts and possible re-activation;
d) deviations from standard tariffs;
e) monitoring of accounts and customer information;
f) RMA exchange operation with the correspondent bank;
g) management of account or other product usage anomalies.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)
- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000)
- Hiding or destroying account documents (Article 10 of Legislative Decree no. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000)

By way of example, this offense could occur if the Branch omits or improperly performs verification and monitoring activities with respect to customers for opening current accounts by proceeding to

authorize the operations of individuals who have been reported to have engaged in tax anomalies.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Credit Manual
- Financial Crime Policy
- Banking business manual
- Charter of Credit Committee
- Suspicious Transaction Reporting Procedure
- Internal Operation and Management Authorization
- BRAINS Manual
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Anti Internal Fraud Policy
- General Governance Policy of ICBC Milan Branch
- Gifts and Entertainment Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Conduct
- Code of Ethics
- Staff Handbook

1.3.10 Credit-related activities

This Risk Activity concerns processes related to:

a) management of the credit appraisal, assessment of credit requirements and collateral and decision-making for the purpose of granting credit;
b) granting of credit and/or various forms of credit facilities;
c) monitoring of financing and possible re-scheduling/suspension;
d) credit termination;
e) conflict of Interest Management and Internal Reporting.

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000)

- Fraudulent declaration through other artifices (Article 3, Legislative Decree No. 74/2000)
- Unfaithful declaration (Article 4, Legislative Decree 74/2000)
- Issuance of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000)
- Hiding or destroying account documents (Article 10 of Legislative Decree no. 74/2000)
- Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000)

By way of example, this offense could occur if the Branch produces altered documents in order to provide financing without the credit requirements being met to customers who have been reported to have engaged in tax anomalies.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Model, are required to strictly observe the following internal regulations adopted by the Branch:

- Tax Affair Management Procedure
- CRS procedure
- Dac-6 procedure
- Credit Manual
- Financial Crime Policy
- Financial Accounting Manual
- Charter of Credit Committee
- Banking Business Manual
- CIB Business Manual
- AML & Compliance Committee Charter
- AML-CTF Due Diligence and Client Onboarding Procedure
- Suspicious Transaction Reporting procedure
- Anti Internal Fraud Policy
- Complaint handling procedure
- Conflict of interest Policy
- General Governance Policy of ICBC Milan Branch
- Internal Operation and Management Authorization
- Market Abuse Policy
- Treasury manual
- Whistleblowing Policy
- Anti-Bribery and Corruption Policy
- Procedure for Assessment and Approval of New Product
- Gifts and Entertainment Policy

- Code of Conduct
- Code of Ethics
- Staff Handbook

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. formal identification of persons charged with roles and responsibilities in tax compliance management;
2. checks for completeness, correctness and accuracy of documentation and information supporting the determination and related payments of direct and indirect taxes;
3. monitoring of deadlines related to the preparation and submission of tax documentation;
4. archiving of accounting documentation;
5. checks on the accuracy of accounting for invoices receivable and payable;
6. clear identification of the people/departments in charge of the purchase of goods and services and the awarding of professional appointments;
7. properly formalized requests for proposals addressed to suppliers;
8. archiving of documentation related to contracts with suppliers;
9. transparent and reconstructible decision-making processes over time related to the conditions stipulated with customers;
10. definition of the methods and criteria underlying any changes and/or renewals of the conditions stipulated with customers;
11. definition of controls on potentially anomalous transactions, in terms of amount, type, object or frequency;
12. implementation of all actions of an organizational-accounting nature necessary to extract the data and information for the correct compilation of reports and their timely submission to the Tax Authority, in accordance with the procedures and timeframes established by the applicable regulations;
13. tracking of intercourse with officials of the Tax Authority for the fulfillment of obligations related to the Branch's business operations and/or as a result of audits/inspections/assessments;
14. archiving and preservation of the documentation produced as part of the management of relations with the Tax Authority;
15. provision for reporting procedures to counter tax evasion;
16. prompt identification of vulnerabilities of systems;
17. traceability of access and critical activities carried out through the Branch’s IT systems;
18. periodic monitoring/control activities on the operations of the Branch also by the SB;
19. appropriate system for sanctioning non-compliance with the measures indicated in the Model:

20. staff awareness activities in the areas of the Branch's operations.

NINETEETH SECTION - CRIMES AGAINST CULTURAL HERITAGE

1.1. Introduction

This Section covers the crimes provided for in Articles 25-septiesdecies and 25-duodevicies of the Decree, added by Law 22/2022 i.e., the crimes provided regarding cultural heritage.

By Law No. 22 of March 09, 2022, "Provisions on crimes against cultural heritage," Title VIII-bis "Of crimes against cultural heritage" was added to the Criminal Code after Title VIII of Book Two for the protection and preservation of cultural heritage and in the fight against illicit trafficking in works of art.

The same law expanded the offenses under Legislative Decree 231/01 with the inclusion after Article 25-sexiesdecies of Articles 25-septiesdecies (Crimes against cultural heritage) and 25-duodevicies (Laundering of cultural property and devastation and looting of cultural property).

Specifically, the cultural heritage crimes covered in Articles 25-septiesdecies and 25-duodevicies of the Decree include:

Art. 25-septiesdecies:

- **Theft of cultural property (Art. 518-bis of the Criminal Code)**: anyone who takes possession of another person's movable cultural property, removing it from its owner, in order to gain profit for himself or others, or takes possession of cultural property belonging to the State, insofar as it has been found underground or on the seabed, shall be liable for this offense.
- **Misappropriation of cultural property (Art. 518-ter of the Criminal Code)**: anyone who, in order to procure an unjust profit for himself or others, appropriates another person's cultural property of which he has possession for any reason is liable for this crime.
- **Receiving of cultural property (Article 518-quater of the Criminal Code)**: anyone who, except in cases of complicity, in order to procure a profit for himself or others, purchases, receives or conceals cultural property originating from any crime, or otherwise meddles in having it purchased, received or concealed, shall be liable for this crime.
- **Forgery in a private writing relating to cultural property (Article 518-octies of the Criminal Code)**: anyone who forms, in whole or in part, a false private writing or, in whole or in part, alters, destroys, suppresses or conceals a true private writing, in relation to movable cultural property, in order to make its provenance appear lawful, shall be liable for this offense.
- **Violations of alienation of cultural property (Article 518-novies of the Criminal Code)**: liable for this offense is:

1) anyone who without the prescribed authorization alienates or places cultural property on the market;
2) anyone who, being obliged to do so, does not submit within the period of thirty days the report of the acts of transfer of ownership or possession of cultural property;
3) the alienator of a cultural property subject to pre-emption who makes delivery of the thing pending the sixty-day period from the date of receipt of the report of transfer.

- **Illegal importation of cultural property (Article 518-decies of the Criminal Code)**: anyone who, outside the cases of complicity in the crimes provided for in Articles 518-quater 518-quinquies 518-sexies and 518-septies, imports cultural property originating from a crime or found as a result of research carried out without authorization where provided for by the law of the State in which the finding took place or exported from another State in violation of the law on the protection of the cultural heritage of that State is liable for this crime.
- **Illicit exit or export of cultural property (Article 518-undecies of the Criminal Code)**: anyone who transfers abroad cultural goods things of artistic historical archaeological ethno-anthropological bibliographic documentary or archival interest or other things subject to specific protection provisions under the regulations on cultural goods without a certificate of free movement or export license or anyone who fails to return to the national territory at the expiration of the term cultural goods things of artistic historical archaeological ethno-anthropological bibliographic documentary or archival or other things subject to specific protection provisions under the regulations on cultural property for which temporary exit or export has been authorized, as well as against anyone who makes false statements in order to prove to the competent export office in accordance with the law that things of cultural interest are not subject to authorization to leave the national territory.
- **Destruction, dispersal, deterioration, defacement, defacement, and illegal use of cultural or scenic property (Art. 518-duodecies, Criminal Code)**: anyone who destroys, disperses, deteriorates or renders wholly or partially unusable or unusable cultural or scenic property belonging to him or to others, or anyone who, outside the above cases, defaces or defaces cultural or scenic property belonging to him or to others, or destines cultural property to a use incompatible with its historical or artistic character or detrimental to its preservation or integrity, shall be liable for this offense.
- **Counterfeiting of works of art (Art. 518-quaterdecies, Criminal Code):** liable for this offense is:
  1) anyone who, in order to make a profit, counterfeits, alters or reproduces a work of painting, sculpture or graphics or an object of antiquity or historical or archaeological interest;
  2) anyone who, even without having participated in the counterfeiting, alteration or reproduction, places on the market, holds for trade, introduces into the territory of the

State for this purpose or otherwise places in circulation, as authentic, counterfeited, altered or reproduced specimens of works of painting, sculpture or graphics, objects of antiquity or objects of historical or archaeological interest;

3) anyone who, knowing them to be false, authenticates counterfeited, altered or reproduced works or objects indicated in Nos. 1) and 2).
4) anyone who, by means of other statements, expert opinions, publications, affixing stamps or labels, or by any other means, accredits or helps to accredit, knowing their falsity, as authentic works or objects indicated in Nos. 1) and 2) that have been counterfeited, altered or reproduced.

Art. 25-duodevicies:

- **Laundering of cultural property (Art. 518-sexies of the Criminal Code):** outside the cases of concurrence, anyone who replaces or transfers cultural property resulting from a non-negligent crime, or carries out other transactions in relation to it, in such a way as to hinder the identification of its criminal origin, shall be liable for this crime.
- **Devastation and looting of cultural and landscape goods (Art. 518-terdecies of the Criminal Code):** liable for this crime, anyone who, outside the cases provided for in Article 285, commits acts of devastation or looting targeting cultural or landscape goods or cultural institutions and places.

1.2. General rules of conduct

Risk Activities must be carried out in compliance with applicable laws, the rules set forth in this Model and, also but not limited to, the provisions of the Code of Ethics and the Code of Conduct, an expression of the values and policies of the Branch.
Actions, operations carried out on behalf of the Branch must be guided by the principles of:

- separation of roles and responsibilities within the Branch;
- fairness, completeness and transparency of information;
- formal and substantive legitimacy;

in accordance with current regulations and according to established procedures.

Branch employees involved in the management of Risk Activities are required, in order to prevent the occurrence of the offenses in question, to comply with the following general principles of conduct:

- to abstain from engaging in conduct such as to integrate the types of offenses considered above (Article 25- duodevicies of the Decree);
- to abstain from engaging in or adopting behaviors and/or acts that are prodromal to the subsequent realization of the types of offenses indicated in this Section.

Recipients of the Model are required to promptly report any potential any potential crime against the cultural heritage of which they become aware.

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes

On the basis of the legislation currently in force and of the analyses carried out, the activities in which the risk of unlawful conduct in relations with crimes against cultural heritage is generally higher concern the Public Administration relationship.

1.3.1 Public Administration relationship

This Risk Activity concerns processes related to:

a) management of relations with Chambers of Commerce;
b) managing relations with Local Public Bodies in charge of waste disposal;
c) management of relations with Government, Regional, Municipal or Local Public Administrations (A.S.L., Fire Brigade, Arpa, etc.) for the execution of fulfilments regarding hygiene and safety and/or authorisations, permits, concessions;
d) relations with the Public Administration in connection with requests for authorisations or performance of fulfilments;
e) management of relations with the Ministry of Economy and Finance, Tax Agencies and Local Public Bodies for the purposes of carrying out tax obligations;
f) management of relations with the Prefettura, the Public Prosecutor's Office ;
g) dealings with public security authorities (Carabinieri, Police, Municipal Police/Local Police, Guardia di Finanza);
h) management of relations with Public Entities for the purposes of compliance with labour and social security laws (e.g. INPS, INAIL, Provincial Labour Directorate, Employment Department, Occupational Medicine, Revenue Agency, Local Public Bodies, etc.);
i) relationships with public clients or private companies owned by public entities;
j) funded training activities (staff training using public contributions).

The types of crime that are abstractly applicable and the related methods of committing them are listed below:

- Theft of cultural property (art. 518-bis, Criminal Code)
- Misappropriation of cultural property (art. 518-ter, Criminal Code)
- Receiving stolen cultural property (art. 518-quater, Criminal Code)
- Illicit importation of cultural goods (art. 518-decies, Criminal Code)
- Illicit exit or export of cultural goods (art. 518-undecies, Criminal Code)
- Laundering of cultural goods (art. 518-sexies, Criminal Code)

By way of example, this offense could occur in the event that the Branch imports/exports goods of artistic historical, archaeological, bibliographic, documentary interest or other things subject to specific protection provisions under the regulations on cultural property without the prescribed authorizations issued by the Public Administration.

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Model, are obliged to strictly observe the following internal regulation adopted by the Branch:

- Financial Crime Policy
- Anti-Bribery and Corruption Policy
- General Governance Policy of ICBC Milan Branch
- Operating Expense Management Rules
- Third-party Management Procedure
- Gifts and Entertainment Policy
- Training Policy
- Whistleblowing Policy
- Conflict of interest Policy
- Code of Ethics
- Code of Conduct
- Staff Handbook

1.4. Mitigation factors

The control system protecting the processes described is based on the following mitigation factors:

1. clear identification of the persons in charge of interfacing with the Public Administration and providing suitable and appropriate documentation against the requests received;
2. formalization of every agreement/convention/contract with public entities in a document, duly signed by individuals with appropriate powers according to the system of powers and proxies in place;
3. traceability of intercourse with officials of the Public Administration for the fulfillment of obligations related to the exercise of the Branch's activities and/or as a result of audits/inspections/investigations;
4. filing and preservation of the documentation produced in the context of the management of relations with the Public Administration;
5. checks for completeness, correctness and accuracy of information transmitted to the Public Administration;

6. periodic monitoring/control activities on the operations of the Branch also by the Surveillance Body;
7. appropriate system for sanctioning non-compliance with the measures indicated in the Model;
8. staff awareness activities in the areas of the Branch's operations.

ANNEXES

- Annex 1 - Risk Assessment & Gap Analysis