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 August 2021

Definitions 1
Acronyms 3
GENERAL PART 1
CHAPTER 1 - THE REGULATORY FRAMEWORK 2
1.1. Introduction 2
1.2. Perpetrators of the Predicated Offence(s) 2
1.3. The Predicate offences for corporate liability 3
1.4. Penalties 4
1.5. Exemption from administrative liability 5
1.6 Crimes committed abroad 5
1.7 Contents of the Models 6
CHAPTER 2 - THE ORGANISATIONAL STRUCTURE AND CORPORATE OPERATION OF THE BRANCH 6
2.1. The Branch 6
2.2. The main area of operation of the Branch 7
2.3. The corporate governance of the Branch 7
2.3.1. Responsibilities of Departments 8
2.3.2 Committees 10
2.3.3 The internal control system 12
2.3.4 Reporting of Internal Control Function 12
2.4 The Organisational, Management and Control Model of the Branch: structure and summary 13
2.5 The procedure to adopt the Model and its subsequent update 14
CHAPTER 3 - THE SURVEILLANCE BODY 15
3.1 Identification of the Surveillance Body 15
3.2. The Surveillance Body 15
3.2.1. Composition, appointment, duration and remuneration of the Surveillance Body 15
3.2.2 Requirements 16
3.2.2.1 Subjective requirements of eligibility 16
3.2.2.2 Autonomy and independence 17
3.2.2.3 Professionalism 17
3.2.2.4 Continuity of action 17
3.2.3 Grounds for disqualification from office 18
3.2.4 Grounds for suspension and termination 18
3.2.5 Duties of the Surveillance Body 19
3.2.6 Control of the adequacy and compliance of the Model 20
3.2.7 Powers of the Surveillance Body 21

3.2.8 Information flows to the Surveillance Body 22
3.2.8.1 Information duties relating to official acts 22
3.2.8.2 Reports from employees of the Branch or Third parties 23
3.2.9 Reporting by the Surveillance Body towards the Board of Directors of Headquarters 23
3.2.10 The internal system for reporting violations (Whistleblowing) 24
CHAPTER 4 - INTERNAL TRAINING AND COMMUNICATION 25
4.1 Introduction 25
4.2. Internal communication and communication to external parties 26
CHAPTER 5 - THE DISCIPLINARY SYSTEM 26
5.1 General Principles 26
5.2 Employees without managerial positions 28
5.3 Managers 29
5.4 External parties 29
SPECIAL PART 30
Introduction to the Special Part of the Model 31
FIRST SPECIAL PART - OFFENCES AGAINST THE PUBLIC ADMINISTRATION 32
1.1. Introduction 32
1.2. General rules of conduct 33
1.3 Risky Activities pursuant to Legislative Decree no. 231/01 and main methods of committing offences 35
1.3.1 Management of the staff selection and recruitment process 35
1.3.2 Relationships with public social security and welfare organizations (e.g. INPS, INAIL) 36
1.3.3 Management of gifts and entertainment 37
1.3.4 Customer relationships 38
1.3.5 Expense Management 39
1.3.6 Second level checks and controls 40
1.3.7 Third level checks and controls 41
1.3.8 Customer complaints management 42
1.3.9 Management of the legal risks 43
1.3.10 Procurement of goods and services 44
1.3.11 Appointment and relations with professional consultants 45
1.3.12 Management of litigation and out-of court settlements 45
1.3.13 Management of relations with the Supervisory Authorities and/or tax Authorities 46
SECOND SPECIAL PART - COMPUTER CRIMES AND UNLAWFUL DATA PROCESSING 48
1.1. Introduction 48

1.2. General rules of conduct 48
1.3 Risky activities pursuant to Legislative Decree no. 231/01 and main methods of committing offences 50
1.3.1 Expense Management 51
1.3.2 Management of information systems and licenses of the software in use 52
1.3.3 Use of Branch goods and services and involvement in the purchase of the same 54
1.3.4 Management of data 55
THIRD SPECIAL PART - ORGANIZED CRIME OFFENCES 57
1.1. Introduction 57
1.2. General rules of conduct 58
1.3 Risky Activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 58
1.3.1 Disbursement of loans granted by the Branch 58
FOURTH SPECIAL PART - CRIMES AGAINST INDUSTRY AND TRADE 59
1.1. Introduction 59
1.2. General rules of conduct 60
1.3 Risky Activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 61
1.3.1 Marketing of banking / financial products 61
FIFTH SPECIAL PART - CORPORATE OFFENCES 62
1.1. Introduction 62
1.2. General rules of conduct 62
1.3 Risky Activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 64
1.3.1 Management of conflict of interests 64
1.3.2 Management of the credit rating 66
1.3.3 KYC and credit assessment 67
1.3.4 Operating expense management 67
1.3.5 Employee management 68
1.3.6 Payments and reimbursements 69
1.3.7 Trade finance business 70
1.3.8 Transaction and payment monitoring 71
1.3.9 Account management 72
1.3.10 Reporting 73
1.3.11 Relations with Financial Intermediaries 73
1.3.12 Customers' account management and periodic monitoring 74
1.3.13 Developing marketing and sales strategies 76
1.3.14 Credit Management 77
1.3.15 Credit rating process 78

1.3.16 Accounting 79
1.3.17 Reliability and integrity of accounting and management information 80
1.3.18 Management of requests related to data processing 81
1.3.19 Second level checks and controls 82
1.3.20 Third level checks and controls 84
1.3.22 Customer complaints management 84
1.3.21 KYC and transaction monitoring 85
1.3.22 Management of the corporate reporting 86
1.3.23 Reporting to Supervisory Authorities 87
1.3.24 Management of relations with the Supervisory Authorities 88
1.3.25 Management of litigation and out-of court settlements 89
SIXTH SPECIAL PART - CRIMES FOR THE PURPOSES OF TERRORISM OR SUBVERSION OF THE DEMOCRATIC ORDER 90
1.1. Introduction 90
1.2. General rules of conduct 91
1.3. Risky activities pursuant to Legislative Decree no. 231/01 and the main modalities for committing crimes 92
1.3.1 Customers' relationship management and periodic monitoring 92
1.3.2 KYC and transaction monitoring 93
1.3.3 KYC and credit assessment 95
1.3.4 Transaction and payment monitoring 96
1.3.5 **AML/CTF Due Diligence and Client Onboarding Procedure** 97
SEVENTH SPECIAL PART - CRIMES AGAINST INDIVIDUALS 98
1.1. Introduction 98
1.2. General rules of conduct 99
1.3 Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 100
1.3.1 Management of the staff selection and recruitment process 100
EIGHTH SPECIAL PART - MARKET ABUSE 101
1.1. Introduction 101
1.2. General rules of conduct 102
1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 103
1.3.1 Management of the restricted information 103
1.3.2 KYC and credit assessment 105
1.3.3 Relations and information flows with Headquarters 106
1.3.4 Relations with Financial Intermediaries 106
1.3.5 Credit rating process 107
1.3.6 Internal dealing regarding privileged information acquired through the credit process 108

1.3.7 Management of the corporate reporting 109
NINTH SPECIAL PART - WORKPLACE HEALTH AND SAFETY OFFENCES 110
1.1. Introduction 110
1.2. General rules of conduct 111
1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 111
1.3.1 Responsible for security 112
TENTH SPECIAL PART - CRIMES CONCERNING RECEIPT OF STOLEN GOODS, MONEY LAUNDERING AND USE OF MONEY, GOODS OR BENEFITS OF UNLAWFUL ORIGIN, AS WELL AS SELF-LAUNDERING 112
1.1. Introduction 112
1.2. General rules of conduct 114
1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 116
1.3.1 Operation and Management Authorization 116
1.3.2 Monitoring of operations and dealing 117
1.3.3 Credit Approval Authority 118
1.3.4 AML/CTF Due Diligence and Client Onboarding Procedure 119
1.3.5 KYC and transaction monitoring 120
1.3.6 KYC and credit assessment 122
1.3.7 Operating expense management 123
1.3.8 Trade finance business 123
1.3.9 Transaction and payment monitoring 124
1.3.10 Account management 125
1.3.11 Management and collection of liquidity 127
1.3.12 Customer relationships 128
1.3.13 Accounting 128
1.3.14 Management of relations with the financial administration (including Tax Authorities) 129
1.3.15 Verification and monitoring on accounting data 130
1.3.16 Appointment and relations with professional consultants 131
1.3.17 Procurement of goods and services 132
ELEVENTH SPECIAL PART - CRIMES INVOLVING BREACH OF COPYRIGHT 132
1.1. Introduction 132
1.2. General rules of conduct 133
1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 134
1.3.1 Use of Branch goods and services and involvement in the purchase of the same 134
1.3.2 Management of the credit files 135

TWELFTH SPECIAL PART - INDUCEMENT NOT TO MAKE OR TO MAKE FALSE STATEMENTS TO JUDICIAL AUTHORITIES 136

1.1. Introduction 136

1.2. General rules of conduct 136

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 137

1.3.1 Management of the participation to the judicial and out-of-court litigation 137

THIRTEENTH SPECIAL PART - CRIMES OF EMPLOYMENT OF THIRD-COUNTRY CITIZENS WHOSE STAY IS IRREGULAR 138

1.1. Introduction 138

1.2. General rules of conduct 138

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 139

1.3.1 Management of the staff selection and recruitment process 139

FOURTEENTH SPECIAL PART - RACISM AND XENOPHOBIA 140

1.1. Introduction 140

1.2. General rules of conduct 140

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 140

1.3.1 Employee management 141

1.3.2 Management of the staff selection and recruitment process 141

FIFTEENTH SPECIAL PART - TRANSNATIONAL OFFENCES 142

1.1. Introduction 142

1.2. General rules of conduct 143

1.3. Risky activities pursuant to Legislative Decree 231/2001 and the main modalities for committing crimes 143

1.3.1 Activities related to the participation in the credit process 143

SIXTEENTH SPECIAL PART - TAX PREDICATED OFFENSES 145

1.1. Introduction. 145

1.2. General rules of conduct 148

1.3. Activities classifiable at risk pursuant to Legislative Decree 231/01 and the main methods of committing crimes. 152

1.3.1 Management of the administrative and accounting structure and the authorization for the sale of significant assets and / or the approval of significant financial transactions. 152

1.3.2 Management of the proposition of new products, services or activities (authorization powers) of the Branch. 154

1.3.3 Developing marketing and sales strategies 156

1.3.4 Management of both the active and passive cycle of accounting and tax declarations. 157

1.3.5 Management of the reliability and integrity of accounting and management expenses and information. 159

1.3.6 Management of customer relations and operations. 160

1.3.7 Management of the reporting to the Tax Authority (including those provided by the international cooperation) and cross-border activities. 162

1.3.8 Management of second level controls 164

1.3.9 Management of third level controls and audits. 166

ANNEXES 168

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, including 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 87/88, Via dei Due Macelli, Rome;
- "**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 Headquarters 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;
- **"Matrix of Risks":** a map that summarizes, for each Department of the Branch, the activities considered at risk for the commission of certain Predicate offences laid down by the Decree and the relative preventive measures adopted by the Branch. The Matrix of Risks of the Milan Branch is attached as Annex 1;
- "**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;
- **"Parent Company":** the Parent Company of the Headquarters is "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 Areas**": Departments 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 "Risk Areas" in the Matrix of Risks of the Branch;

- **"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 "Description of the Activities" in the Matrix of Risks 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;
- **"Trade Association":** an association that represents and protects the interests of all people that exercise the same economic or work activity, public or private.

Acronyms

- **"AML/CTF"**: Anti-Money Laundering and Counter Terrorism Financing
- "**CIB":** Corporate & Investment Banking Department
- "**CONSOB**": National Commission for Companies and Stock Exchange
- "**FI**": Financial Institutions Department
- **"GM":** General Management
- "**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
- **"UIF"**: Financial Intelligence Unit
- **"HQ":** Headquarter

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 administrative liability of entities is to be considered further and independent from the criminal liability recognized at the individuals who have committed the crime.

The entity's administrative liability lies beyond and is different from that of the natural person who materially commits the offence and they are both subjected to investigation in the same proceeding before a criminal court. 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. 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 liability for corporate offences resulting from crimes is normally ascertained as part of the same criminal proceedings relating to the natural person committing the crime. The Decree introduced new elements in the Italian legal system, as penalties of both a monetary nature and consisting of prohibitions in relation to crimes committed by persons functionally related to Entities are now applicable to those entities.

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 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-Manger” 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. Crimes involving breach of copyright (referred to in article 25-novies of the Decree);
14. The crime of “Inducement not to make or to make false statements to judicial authorities”

(referred to in article 25-decies of the Decree);

15. Offences against the environment (referred to in article 25-undecies of the Decree);

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

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

18. Fraud in sporting competitions, illegal practice in gambling sector and through banned means (referred to in article 25-quaterdecies[1]);

19. Tax Predicated Offence (referred to in article 25-quinquiesdecies)[2];

20. Smuggling (referred to in art. 25-sexiesdecies)[3];

21. 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");

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

23. Fraud against the European Agricultural Fund (L. No. 898/1986, Article 2)[4].

A comprehensive list of the relevant crimes applicable to the Branch is attached to this document under Annex 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[5]") 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

[1] As implemented by L. No. 39/2019 Fraud in sports competitions (L. No. 401/1989 art. 1)
[2] As introduced by L. No. 157/2109 and amended by L.D. No. 75/2020.
[3] As introduced by L.D. No. 75/2020 referring to DPR No. 43/1973 articles 282; 283; 284; 285; 286; 87; 2888; 289; 290; 291; 291.bis; 291.ter; 291-quarter; 292; 295;.
[4] As introduced by L. D. No. 75/2020 and classified and implemented as Predicated Offences limited to entities operating in the olive oil business sector: ref. to articles of the criminal code as per 440; 442; 444; 473; 474; 515; 517; 517-quarter.
[5] 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.

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;
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

According to the Decree, if the offence is committed by a Senior Person, 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;
- define the procedures through which the Entity makes and implements decisions relating 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.

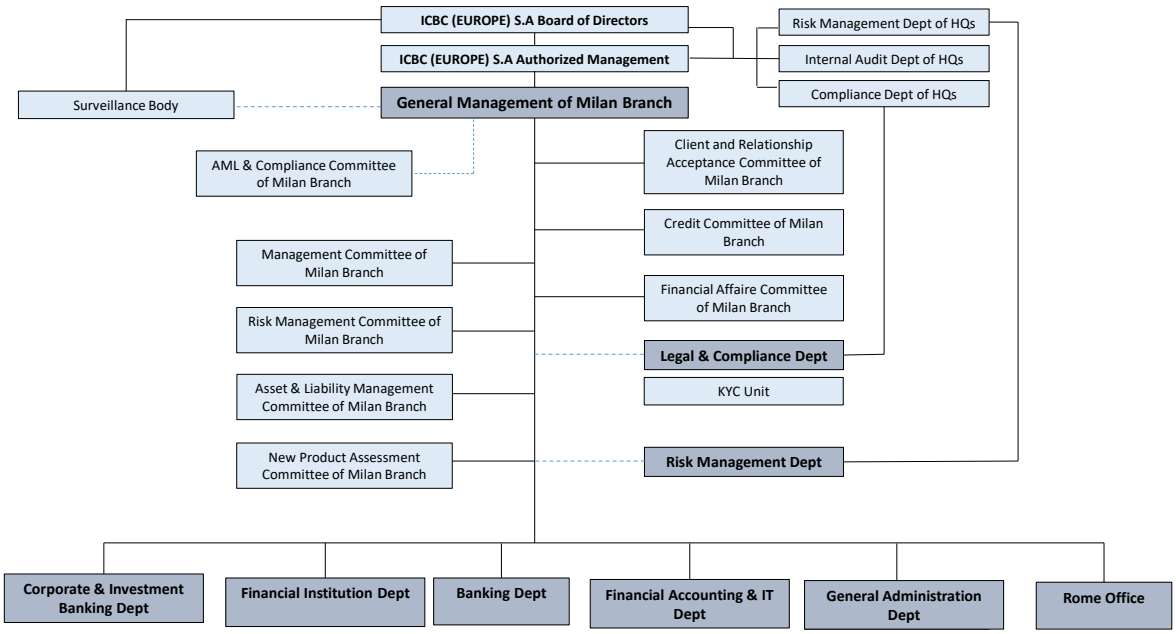
This Model was drafted and updated also having regard to the Guidelines. Any misalignments of any provision of this Model from the principles set out in the Guidelines has been evaluated and assessed having regard to, among others, the actual organization of the Branch and the Headquarters and the relevant 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 a branch of ICBC (Europe) S.A. 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 Headquarters 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 Parent Company 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[6]:

[6] 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 Headquarters in Luxembourg.



Note: the continuous lines indicate the hierarchical and functional reporting, while the blue dotted lines indicate the functional reporting.

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. With the business scope covering commercial banking business and investment banking business, the Branch provides its clients with several financial services including international settlement, time deposit, corporate loan and trade finance.

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:

- world top 500 companies and local top 50 listed companies, advanced manufacturing companies, top Chinese enterprises in Italy and customers involved in local major M&A projects;
- top-rated customers with stable and adequate cash flow, lowly affected by economic cycles;
- companies with strong internationalization and low level of revenue concentration and companies with an external rating higher than the Italian Government rating;
- primary Chinese companies investing overseas;
- Italian banks.

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 of relations 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

The management of the Branch 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 Headquarters 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 for the different functions (business, support and control) as well as for the different business units (services, departments or positions) their structure and the reporting and functional lines with the General Management and the Headquarter.

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 in charge for the management of retail customer fund claim operations 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 Headquarters and by the Parent Company 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 and testing support. In addition, responsibilities of the IT function include taking charge of data protection at the Branch level. Be the Data Protection Coordinator (DPC) at the Milan Branch towards the Data Protection Officer (DPO) and the local senior management to implement the data protection controls of the Branch; Identify and monitor the risk with data protection regulations; Conduct the departments to implement procedures, risk assessments and action plans to ensure the level of compliance of the Branch with data protection.

Risk Management Department is an internal 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 Headquarters 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 delegate 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 Headquarters 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 is in charge to discuss the Branch's strategy and other relevant issues concerning the Branch. It takes place once a month.

The Risk Management Committee is composed of the General Management, the Heads and the Deputy Heads of all Departments. The Committee is the decision-making organization on the overall risk management of the Branch. The Committee deliberates collectively the significant events of overall risk management, the policies and procedures on internal control, etc.. In addition, the Committee also performs the duty of the IT Management Committee of the Branch. It takes place at least once every quarter.

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. The Credit Committee supports the decision-making of the General Management in credit risk management. The Committee collectively reviews the financing, investment and other operations that shall be examined and approved by the Branch according to credit risk examination and approval procedures, provides the decision-making basis for the authorized approver(s), and reports to the General Management. It takes place when business needs arise.

The Client Relationship Acceptance Committee 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/her back-up. Other non-voting member invitees (such as staff of the Legal and Compliance Department, staff of the KYC Unit and of business department presenting the prospect/client) may be invited on a case by case basis. The Committee has the general responsibility to assess and accept all types of "High AML risk clients" and monitor in compliance with the AML Risk Appetite Framework the limit sets concerning financial engagement (loan), any form of financial commitment or any flows of transaction.

The Anti-Money Laundering & Compliance Committee is composed of the General Management, the Head of the Legal & Compliance Department, the Head of the Risk Management and the back-up money laundering reporting officer. The Anti-Money Laundering & Compliance Committee is in charge for (i) overseeing the Branch's implementation of compliance program, policies and procedures that are designed to respond to the various compliance and regulatory risks; (ii) reporting to the General Management (and to the Headquarter, to which the minutes of each meeting are sent) the general status of the anti-money laundering and suspicious transactions reporting of the Branch and (iii) perform any other duties as directed by Headquarter. It takes place once a month.

The Financial Affairs Committee is composed of the Deputy General Manager in charge for financial accounting and the Heads of the Financial Accounting & IT Department, General Administration, Banking, Financial Institutions, Risk Management, Corporate & Investment Banking and Legal & Compliance Department. The committee is mainly responsible for the discussion and approval of Branch's major financial matters and monitoring the implementation of the important financial project. In general, the scope of the committee includes the approval of single transaction at the amount over Euro 15,000.00 and other specific relevant financial expenditures.

The Asset & Liability Management Committee is composed of the General Management and the Heads of the Risk Management, Financial Accounting & IT, Corporate & Investment Banking and Financial Institutions Departments. This Committee is in charge of the discussion and analysis of

every question relating to the asset and liability management. It takes place at least once every quarter.

The New Product Assessment Committee is composed of the Deputy General Managers and the Heads of the Risk Management, Legal & Compliance, Financial Accounting & IT, Banking, Corporate & Investment Banking and Financial Institutions Departments. The New Product Assessment Committee reviews the new product application according to new product assessment and approval procedures, provides the decision-making basis for General Manager of the Branch, and reports to General Manager of the Branch. It meets when the approval of a new product needs to be assessed.

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 among others specific reports on a regular basis (monthly, quarterly and annual) and in case of events, towards the General Management of the Branch and the Legal & Compliance Department/Chief Compliance Officer of Headquarter. Based on the standards required by the Headquarters and the templates drawn up by the Departments, the reporting provides qualitative and quantitative information on the activities performed, the identified shortcomings and corrective actions aimed at restoring compliance with the legislation.

The Risk Management Department informs the Headquarters periodically and in case of events regarding the regulatory risk indicators (Capital Requirements, Large Exposure Limit, Liquidity Coverage ratio, Net Stable Financing ratio, etc) and risk limits, the quality of lending activities, the market risk exposure and the operational risk indicators.

As mentioned, the Internal Audit tasks are performed on the Branch directly by the Internal Audit Department of the Headquarters on the basis of an independent audit planning. In particular, at least once a year, the Internal Audit Department of the Headquarters conducts its audits with reference to the adequacy of procedures and risk profiles of the Branch.

The results of the audit activities and the related operative indications are documented in a report addressed to the General Management of the Headquarters and to the General Management of the Branch. This report also provides a description of the corrective actions aimed at solving and/or preventing the findings identified.

In this framework, the Risk Management Department of the Branch operationally supports the Internal Audit Department of the Headquarter and the relevant Departments of the Branch in the monitoring and implementation of the corrective measures.

2.3.4 Reporting of Internal Control Function

Internal Control Function (hereinafter, the “Branch ICF”) refers to the Risk Management

Department and the Legal & Compliance Department of the Branch. The Branch ICF depend, from a hierarchical and functional point of view, on the internal control functions of the Headquarters (hereinafter, the “Headquarters 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.

Reports established by the Branch have to be final and approved in compliance with local and internal rules and have to be applied with a follow up activity about opinions, findings, and recommendations made, in order to comply to all local regulations.

The internal control functions of Headquarter supervise and control the internal control functions of all the Branches. The internal control functions of Headquarter shall pay attention that the shortcomings, irregularities and risks identified throughout the whole bank are reported to the local management in an appropriate way for the information that serves to improve the control environment and the control of risks.

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, in order to identify the related mitigation and preventive measures adopted by the Branch.

The outcome of this activity constitutes the content of the Special Parts 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 steps that allowed the identification of risk areas on the basis of which the Special Parts of this Model were drafted are shown below:

Risk Assessment:

- study of the Branch’s internal documentation and procedures (Organizational Chart, activities, processes, etc.);
- identification of a series of Risky Activities in respect of which the commission of the Predicate offences laid down by the Decree could be supposed;
- drafting of a "Matrix of Risks” for each Department of the Branch, in which Risky Activities that are carried out by each Department, the Predicate offences that could be committed and the related preventive measures adopted by the Branch are identified;
- sharing of the “Matrix of Risks” with all heads of Department of the Branch in order to collect feedbacks on the correctness of the description of the risk activities identified, based on the knowledge and experience of employees of the Branch;
- evaluation of feedbacks received on the “Matrix of Risks”: 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 Sections" 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 Special Sections 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 Headquarters, 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.

The Model is aimed at regulating business organization and 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 Headquarters 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 Special Parts 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 Special Parts 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 Headquarters 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 of the Branch, based on the principles set out in Legislative Decree no. 231/01 and the

principles to which the Branch is inspired, consists of:

- Code of Ethics;
- Model 231 - General Part;
- Model 231 - Special Section;
- Annex 1 – Matrix of risks;
- Annex 2 - List of Updated Predicated Offences.

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 Headquarters' approval.

CHAPTER 3 - THE SURVEILLANCE BODY

3.1 Identification of the Surveillance Body

In accordance with the Decree, the task of monitoring the Model's observance and its updating is 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 Headquarters 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 Headquarters.

In particular, the Board of Directors of Headquarters 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. In case of renewal of the appointment of an existing member of the Surveillance Body, he/she shall provide the Board of Directors of Headquarters with an up-to-date self-declaration.

In the potential event of revocation, forfeiture or other causes of termination of one or more members, the Board of Directors of Headquarters 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[7];
- situations in which autonomy and independence may be seriously compromised[8];
- 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 Headquarters 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.

[7] 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”.

[8] 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.

As mentioned in paragraph 3.2.1 above, each members 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 Headquarters 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 Headquarters a statement of expenses incurred as part of its annual report.

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 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 Branch 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 Headquarters of the occurrence of one of the above-mentioned grounds for disqualification from the office.

The Chairman of the Board of Directors of Headquarters shall immediately inform the other members of the Board of Directors of Headquarters 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 Headquarters 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 Headquarters, 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 Headquarters 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 Headquarters 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 Headquarters 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 Headquarters 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 Headquarters 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 Headquarters, or
- pursuant to a justified resolution or upon a proposal of the Board of Directors of Headquarters, 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;
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 Headquarters 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 Headquarters 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 Headquarters any violation of the Model that is deemed to be founded by the Surveillance Body itself, of which it has become aware of the report by the employees or by the same ascertained;
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 Headquarters 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 Headquarters 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 areas 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 Headquarters;
- 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 Headquarters 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;
- to be promptly provided with all the data and/or information required to identify aspects related 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.

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 Headquarters 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, on a quarterly basis, each Department of the Branch is requested to send to the Surveillance Body an update of the relevant information and material events and circumstances occurred in the previous quarter, by using the template of “Information Flow” prepared and circulated by the Surveillance Body itself.

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 Headquarters.

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, the following provisions apply:

- any reports should be collected regarding violations of the Model or behavior that is not in line with the rules of conduct adopted by the Branch;
- the Surveillance Body will evaluate the reports received at its reasonable discretion and responsibility, listening if necessary to the author of the report and / or the person responsible for the alleged violation. Following this assessment, any decision not to proceed with an external investigation must be motivated in writing;
- the reports must be in writing and not anonymous, and concern any violation or suspected violation of the Model. The Surveillance Body will act in such a way as to ensure the reporters against any form of reprisal, discrimination or penalty. It shall also ensure the confidentiality of the identity of the reporters, without prejudice to legal obligations and the protection of the rights of the Branch or of the persons falsely accused and / or in bad faith;
- in order to facilitate the flow of reports and information to the Surveillance Body, the establishment of "dedicated" information channels is planned.

The reports to the Surveillance Body can be made by E-mail.

The Branch has set up the following e-mail box reserved for sending the reports to the Surveillance Body, the email address is: **OdV@it.icbc.com.cn**

The Surveillance Body can be convened with an urgent meeting in order to examine carefully and promptly the reports of illicit conduct found by the Surveillance Body during its supervisory and control activities.

In any case, each Head of the Departments must inform the Surveillance Body of any anomaly or violation of the Model might be encountered in the context of the checks conducted on the Area/Function within its competence.

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

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 Headquarters.

The Surveillance Body constantly reports to the Board of Directors of Headquarters 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 Headquarters, 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 behaviors through the normal reporting channels (i.e. through their immediate or next higher level manager) in order to keep an open dialogue.

However, in the case of an employee may feel unable or uncomfortable raising a concern through the normal reporting channels, the Whistleblowing procedure 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, including anonymously, a concern outside the normal reporting channels.

The Branch has appointed the Head of Legal & Compliance Department as “Reporting 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”.

The Reporting Officer shall advice the local senior management to request a full investigation. If the senior management does not follow the Reporting Officer’s advice to request a full investigation, the Reporting Officer may escalate to the next higher level Reporting Officer.

In the event that the concern relates to the Head of Legal & Compliance Department, the whistleblower must report the matter to the Chief Compliance Officer in Luxembourg and copy the local senior management.

Without disclosing the identity of the whistleblower, the Reporting Officer shall report the concerns to the direct reporting level of the whistleblower and to the Head of General Administration Department, if deemed appropriate.

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 concerns about actual or suspected irregularity or misconduct of a general, operational or financial nature within the Branch, including but not limited to:

1. Accounting, internal accounting controls or auditing matters (including the offences that can constitute Tax Predicated Offence);
2. Money laundering or terrorist financing;

3. Market abuse;
4. Insider trading;
5. Breach of (client) confidentiality or privacy;
6. Theft;
7. Fraud;
8. Bribery or corruption
9. Working environment
10. Fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Branch;
11. Fraud or deliberate error in the recording or maintaining of financial records of the Branch;
12. Deficiencies in or noncompliance with the Branch's internal accounting controls;
13. Misrepresentations or false statements to or by an officer of the Branch or an accountant regarding a matter contained in the financial records, financial reports or audit reports of the Branch;
14. Deviation from reporting of the Branch's financial condition as required by applicable laws and regulations;
15. Tax anomalies/event of risk/potential Predicated Offences (omitted and or false tax declarations and/or any and all other tax offences constituting crime).

Employees of the Branch are encouraged to report any concerns through:

- e-mail addressed to **whistleblowing@it.icbc.com.cn;**
- an anonymous written document;
- face to face.

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.

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", this course also includes a final test that must be supported and passed, obviously the Branch is aware of the effective participation by the employees.

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.

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.

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 initiation of action on the basis of the reports submitted by the Surveillance Body, the implementation and finalization of the disciplinary proceeding in respect of employees shall be carried out within the limits of its competences by the General Administration Department, after consultation with the General Management.

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 shall mention any disciplinary actions taken against employees during the reporting period in the "Information Flow" template to be 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 Areas, 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 Areas, 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 activities

belonging to the Risky Areas, 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.

Where the Model is infringed by members of the Management Committee, the Surveillance Body shall so inform the Management Committee, which shall adopt the initiatives it deems appropriate having regard to the nature of the infringement, in accordance with the current legislation.

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 Part (hereinafter also referred to as the "Special Part") is 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.

As already highlighted, the Model is composed of a "General Part" - relating to regulatory framework, the organization structure and corporate operation of the Branch, the Surveillance Body, training and disciplinary system - and a "Special Part", which concerns the application of the control framework with specific reference to the types of crime highlighted by Legislative Decree no. 231/2001 that the Branch has taken into consideration, due to the characteristics of its activity.

In consideration of the analysis of the structure, the areas of operation, the Risky Activities and the risk areas of the Branch, all the types of crime included in the Decree could be abstractly realized and however, the following individual Special parts examine and analyze those crimes included in the families of crime that have been identified as particularly relevant.

In addition, with reference to:

- Offences against the environment (referred to in article 25-undecies of the Decree);
- Crimes against female genital mutilation practices (referred to in article 25-quater.1 of the Decree);
- Fraud in sporting competitions, illegal practice in gambling sector and through banned means (referred to in article 25-quaterdecies[9]);
- Smuggling (referred to in art. 25-sexiesdecies)[10];
- Counterfeiting and / or sanitary adulteration (Law No. 9/2013 art. 12);
- Fraud against the European Agricultural Fund (L. No. 898/1986 . Article 2)[11].

the Branch considered that the risk of committing such crimes is only abstractly and not concretely conceivable and, in any case, external to the business activity perimeter of the Branch; therefore, its 231 administrative liability is excluded and/or external and/or contrary to the Branch statute and to the banking and financial activities. In any case, the preventive measures adopted by the Branch in order to prevent the crimes detailed in the individual special parts, 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).

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

[9] As implemented by L. No. 39/2019 Fraud in sports competitions (L. No. 401/1989 art. 1)
[10] Are classified and implemented as Predicated Offences limited to entities operating in the olive oil business sector: ref. to articles of the criminal code as per 440; 442; 444; 473; 474; 515; 517; 517-quarter.
[11] As introduced by L. D. No. 75/2020.

- Introduction: dedicated to the description and reference legislation governing the crimes included in that 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 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. This Special Part is intended for all employees of the Branch who, regardless of their role, may be liable, in relation to the duties assigned, for the offences described in the Special Part.

For any other provision not expressly provided for or regulated in the Special Part, please refer to the provisions of the General Part of the Model.

In general, the control system set up by the Branch provides for the control by the Surveillance Body on the suitability and effectiveness of the Model.

The Surveillance Body periodically carries out specific checks on the activities connected with the Risky Areas, in order to verify compliance with the general rules of conduct and internal policies / procedures of the Branch.

In addition, the Surveillance Body must have autonomous powers of initiative and control, as well as access at any time to all relevant documentation of the Branch. Within the scope of its powers, the Body may also convene specific meetings with the persons involved in the management of the Risky Activities and carries out specific controls, based on the reports received, as reported in the General Part of the Model.

FIRST SPECIAL PART - 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.

For the purposes of this Model, Public Administration is defined as being any legal person that pursues and/or implements and manages public interests and which is engaged in legislative, jurisdictional or administrative activity, governed by provisions of public law and which is implemented through instruments issued by the Authorities.

Purely by way of example, and with reference to the entities typically having relations with the

Branch, the following can be identified as being Public Administration Bodies:

- the State, the Regions, the Provinces, the Municipalities;
- Ministries, Departments, Committees;
- Non-economic Public Entities (INPS, INAIL);
- Tax Authority.

Among the types of criminal offences considered here, extortion in office and illegal inducement to give or promise benefits, as well as bribery, in its various forms, assume the involvement of a private individual and a public agent, i.e. a natural person who, for the purposes of criminal law, holds the position of "Public Official" and/or of "Person in Charge of a Public Service", as defined respectively in Articles 357 and 358 of the Criminal Code.

The title of "Public Official" is given to those who perform a legislative, judicial or administrative public function[12].

The title of "Person in Charge of a Public Service" is assigned by exclusion, as it goes to those who perform public interest activities, not consisting of simple or merely material tasks, governed in the same manner as public function, but which do not entail the powers typically assigned to a Public Official. Purely by way of example, we may mention the following persons, who have been identified by case law as being Person in Charge of a Public Service: payment collectors of the National Electricity Company, gas and electricity meter readers, post office clerks tasked with sorting correspondence, employees of the Italian State Mint, security guards responsible for cash consignments.

Under the Criminal Code, the conduct of the private individual – whether as bribe-giver or as the party induced to give or promise benefits − is a punishable criminal offence not only when involving Public Officials and Persons in Charge of a Public Service within the Italian Public Administration, but also when it involves:

- persons holding corresponding functions or performing corresponding activities within European Community institutions, or within Entities established on the basis of the Treaties establishing the European Communities, or, lastly, within the other European Union Member States;
- persons holding corresponding functions or performing corresponding activities within other third countries or international public organizations, provided that, in this case, the private individual pursues an undue benefit for himself or others with reference to an international economic transaction or acts in order to obtain or maintain an economic or financial activity.

1.2. General rules of conduct

In order to operate in compliance with the provisions of law and ethics, payments or fees, in any

[12] The exercise of an administrative public function is usually associated with those who have decision-making responsibilities or concur to the decision making process of a public body or who represent the public body in dealings with third parties, and with those exercising authoritative powers.

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, 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 their supervisor or Head of Legal & Compliance Department.

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

In order to commit the Offences in relations with the Public Administration, it is necessary to establish contractual and non-contractual relations and/or any contact (indirect too) with Public Officials and/or subjects in charge of a Public Service.

Furthermore, in order to correctly assess the risks of committing offences against the Public Administration, it is necessary to consider the types of counterparties that relate to the Branch during the performance of certain activities.

The Branch has carried out an investigation in consideration of the various activities carried out by the Departments and has identified a series of Risky Activities during which the conditions for the commission of the offences in relations with the Public Administration could be created.

In relation to the aforementioned offences, the following are the Risky Activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Management of the staff selection and recruitment process

This risky activity concerns activities related to:

- planning, updating and management of recruiting processes;
- performance monitoring during probationary period, coordination the training of staff;
- elaboration of the request of employees to carry out external business activities and review the conflict management arrangements and compliance with such by respective business areas;
- relationships between employees and solutions to possible conflicts;
- health and safety and workplace risks, in accordance with the contents of Legislative Decree no. 81/2008.

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 Criminal Code 1st paragraph)[13];
- Embezzlement takin profit from other's mistake[14];
- Bribery relating to the exercise of duties (Article 318 of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code[15])

[13] As introduced by L.D. No. 75/2020).
[14] As introduced by L.D. No. 75/2020;
[15] Fines enhanced if committed against the European Union economic interests (L.D. No. 75/2020)

- Incitement to bribery (Article 322 of the Criminal Code[16]);
- Office Abuse (Article 323 of the Criminal Code)[17];
- 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.

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

- Code of Ethics
- Whistleblowing Policy and Procedure
- Staff Handbook
- Code of Conduct of ICBC (Europe) S.A.
- Complaint handling Policy & procedure
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Internal Operation and Management Authorization
- The Administrative Measures for Staff Recruitment of ICBC (Europe) S.A Milan Branch (Principles of selection management; multi-stage recruitment and selection process, independence of selectors)
- Implementation Rules for Operating Expense Management
- Conflict of interest Policy
- Anti-Internal Fraud Policy.

1.3.2 Relationships with public social security and welfare organizations (e.g. INPS, INAIL)

This risky activity concerns management of relationships with public social security and welfare organizations in order to fulfill the obligations established by law, regulations or provisions, the performance of which call for direct relationships with the Public Administration.

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

- Unlawful receipt of public grants to the detriment of the State (Article 316-ter of the Criminal

[16] Including any offence against the European union economic interests (L.D No. 75/2020).
[17] As introduced by L.D. No. 75/2020.

Code[18])

- Embezzlement to the detriment of the State (Article 316-bis of the Criminal Code)
- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Aggravated fraud for the purpose of obtaining public funds (Article 640-bis of the Criminal Code)
- Computer fraud (Article 640-ter of the Criminal Code)
- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code[19])
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)
- Fraud in public supply (Article 356 of the Criminal Code)

By way of example, this offence could be verifying by the promise or pay/offer undue sums of money, gifts or free benefits (outside the scope of practices regarding courtesy gifts of little value) and grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration on a personal basis in order to further or favor the Branch's interests.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Implementation Rules for Operating Expense Management
- Anti-Internal Fraud Policy

1.3.3 Management of gifts and entertainment

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. Employees must obtain pre-approval from their Head of Department

[18] Fines enhanced if committed against the economic interests of the European Union (L. D No. 75/2020).
[19] Including committing actions against the economic interests of the European Union (L. D No. 75/2020).

and notify local Senior Management prior to accepting gifts or entertainments valued above €100. The offering and receiving of reasonable business entertainment may fall outside these requirements.

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

- Unlawful receipt of public grants to the detriment of the State (Article 316-ter of the Criminal Code)
- Embezzlement to the detriment of the State (Article 316-bis of the Criminal Code)
- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Aggravated fraud for the purpose of obtaining public funds (Article 640-bis of the Criminal Code)
- Computer fraud (Article 640-ter of the Criminal Code)
- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, promise or pay/offer undue sums of money, gifts or free benefits (outside the scope of practices regarding courtesy gifts of little value) and grant advantages or other benefits of any kind – directly or indirectly, on one's own behalf or for others − to representatives of the Public Administration on a personal basis in order to further or favour the Branch's interests.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Anti-Internal Fraud Policy

1.3.4 Customer relationships

This risky activity concerns activities related to:

- promote products and services, introduce products and services to the customer and structure the transaction (including intra-EU operations);
- management of the relationship with actual Corporate customers and any other type of counterparties;
- manage and maintain existing customer relationships as well as develop new relationships.

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

- Bribery (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater 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, to speed up current practices, etc.).

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Complaint handling Policy & procedure
- Credit Management Manual
- Anti-Internal Fraud Policy

1.3.5 Expense Management

This risky activity concerns activities related to:

- management, accounting and check of operating expenses;
- Preparing operating expense budget and check whether the expenses are reasonable;
- Check and reports of payments filing, registration approved invoice and reimbursement sheets.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Implementation Rules for Operating Expense Management
- Financial Affairs Committee Working Regulation of ICBC (Europe) S.A. Milan Branch
- Anti-Internal Fraud Policy

1.3.6 Second level checks and controls

The Legal & Compliance Department carries out activities related to:

- carry out second level checks and controls within the Branch;
- measure and assess the non-conformity risk for the Branch, identifying and proposing any necessary remedial actions to mitigate and/or prevent any risk;
- conduct and coordinate any necessary investigation/control, check and investigations related to the Legal and AML Compliance matters.

In addition, regarding the Risk Management Department, the activity concerns:

- organize the Department's work to fulfil comprehensive risk management tasks with respect to identifying, measuring, analyzing, monitoring and reporting of credit risk, liquidity risk, market risk, operational risk and country risk;
- verify the periodic review report sent by Corporate & Investment Banking Department; verify / evaluate CIB Department’s suggestions for loan classifications and provisions;
- prepare credit risk reports according to the requirements of Senior Management and ICBC Europe.

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

listed below:

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)
- Unlawful receipt of public grants to the detriment of the State (Article 316-ter of the Criminal Code)
- Embezzlement to the detriment of the State (Article 316-bis of the Criminal Code)
- Fraud against the State or another public entity (Article 640, paragraph 2, no. 1, of the Criminal Code)
- Aggravated fraud for the purpose of obtaining public funds (Article 640-bis of the Criminal Code)
- Computer fraud (Article 640-ter of the Criminal Code)

By way of example, the crime of bribery for the exercise of the function could be configured in the case of obtaining undue favorable treatment by Supervisory Authorities in exchange for the donation or the promise of benefits.

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

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Internal Operation and Management Authorization
- Code of Conduct of ICBC (Europe) S.A.
- Implementation Rules for Operating Expense Management
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Charter of Credit Committee
- Charter of Risk Management Committee
- Anti-Internal Fraud Policy

1.3.7 Third level checks and controls

The Internal Audit function of ICBC (Europe) S.A. Milan Branch is located to the Headquarters in Luxembourg, and carries out the annually the following activities as part of third-level checks and controls:

- controls the regular performance of operations and the trend of risks;
- identifies anomalous trends, violations of procedures and regulations;
- evaluates the completeness, adequacy, functionality and reliability of the organizational structure and other components of the internal control system;
- brings to the attention of the corporate bodies the possible improvements to the risk management policies and any critical issues or violations found;
- based on the results of its checks, formulates recommendations to the corporate bodies.

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

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the crime of bribery for the exercise of the function could be configured in the case of obtaining undue favorable treatment by Supervisory Authorities in exchange for the donation or the promise of benefits.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and procedure
- Internal Audit Charter of ICBC (Europe) S.A.
- Outsourcing Management Measures of ICBC (Europe) S.A. Milan Branch
- Anti Internal Fraud Policy

1.3.8 Customer complaints management

This risky activity concerns activities related to handle the customer complaints in a timely and sound fashion and to provide the necessary internal and external reporting.

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

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)

- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the offenses under consideration could be realized 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 for compliance or against their official duties (for example not to detect irregularities that emerged during the inspection, to speed up current practices).

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

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Complaint handling Policy & procedure
- Anti Internal Fraud Policy

1.3.9 Management of the legal risks

This risky activity concerns activities related to:

- constantly monitoring and managing the potential legal risk in connection with the business activities carried out by the Branch, also in coordination with the Legal Department of HQ and by establishing good relationship with external law firms;
- management of judicial and extrajudicial litigation, also in connection with external law firms;
- daily legal assistance to relevant departments and review of the agreements to be signed by the Branch.

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

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater 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 if the employee in charge of management of the legal risks offers money, goods or other benefits to another counterpart involved in a claim or

an extrajudicial litigation in order to provide an undue advantage to the Branch.

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

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A.Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Complaint handling Policy & procedure
- Policy on the Management of the external legal advisors
- Policy and procedure concerning the involvement of the legal function in the context of business transactions
- Anti Internal Fraud Policy

1.3.10 Procurement of goods and services

This risky activity concerns activities related to the negotiation / conclusion of contracts for appointments and procurement of goods and services, the execution of works and the assignment of consulting services.

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

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the crime of bribery could be realized in the event that an employee of the Branch offers goods, money or other illicit benefits to suppliers in order to 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.

- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Policy on the Management of the external legal advisors
- Implementation Rules for Operating Expense Management
- Anti Internal Fraud Policy

1.3.11 Appointment and relations with professional consultants

This risky activity concerns activities related to the appointment of professional consultants, in particular intellectual services including qualified consultancy activities, in order to support specific audit activities to carry out at Branch level.

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

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Illegal inducement to give or promise benefits (Article 319-quater of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the crime of bribery could be realized in the event that an employee of the Department offers goods, money or other illicit benefits to suppliers (or consulting and professional services including fiscal and tax services or “tax compliance” too) in order to 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and procedure
- Conflict of interest Policy
- Financial Affairs Committee Operation Regulation (HQ)
- Outsourcing Management Measures of ICBC (Europe) S.A. Milan Branch
- Anti Internal Fraud Policy

1.3.12 Management of litigation and out-of court settlements

This risky activity concerns activities related to all the Branch Structures involved in:

- management of judicial and out-of court litigation (administrative, civil, criminal, tax, labour and social security litigation)

- out-of-court settlements with Public Bodies
- participation in legal proceedings as an active / passive party.

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

- Corruption (Articles 318, 319, 320, 321 and 322 bis of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter, paragraph 1, of the Criminal Code)
- Traffic of illicit influences (Article 346-bis of the Criminal Code)

By way of example, the offense related to corruption could occur if an employee of the Branch promises or delivers some money or other benefits towards a customer involved in a complaint, in order to dissuade him from proceeding judicially towards the Branch.

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

- Code of Ethics
- Code of Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Policy on the management of external legal advisor
- Customer complaints
- Anti Internal Fraud Policy

1.3.13 Management of relations with the Supervisory Authorities and/or tax Authorities

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.

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 European Central Bank
- the Bank of Italy
- Consob
- Data Protection Authority

- Tax Authority.

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

- Bribery relating to the exercise of duties (Article 318 of the Criminal Code)
- Bribery relating to an act contrary to official duties (Article 319 of the Criminal Code)
- Bribery in judicial proceedings (Article 319-ter of the Criminal Code)
- Corruption of a person in charge of a public service (Art. 320 of the Criminal Code)
- Incitement to bribery (Article 322 of the Criminal Code)
- Traffic of illicit influences (Article 346-bis 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 Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Policy on the manage of external inspections
- Suspicious transaction reporting procedure
- Anti Internal Fraud Policy

SECOND SPECIAL PART - 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[20].

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.

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

[20] Introduced by Article 7 of Law 48/2008, concerning the ratification and implementation of the Budapest Council of Europe Convention on Cybercrime.

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 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.

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

This Special Part describes the risk profiles relating to the Predicate offences included in the family of computer crimes and unlawful data processing, and therefore all the crimes listed in article 24-bis of Legislative Decree no.231/01.

In relation to the aforementioned offences, the following are the Risky Activities identified within the

Branch and the main methods of implementation of the same.

1.3.1 Expense Management

This risky activity concerns activities related to:

- management, accounting and check of operating expenses;
- Preparing operating expense budget and check whether the expenses are reasonable;
- Check and reports of payments filing, registration approved invoice and reimbursement sheets.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics

- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Implementation Rules for Operating Expense Management
- Financial Affairs Committee Working Regulation of ICBC (Europe) S.A. Milan Branch
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. Rules of IT General Management
- Information Security Policy
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- Measures of Information and Information System Security Management
- Information System Security Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Milan Branch 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
- Information System User Management Policy of ICBC (Europe) S.A.
- Information System User Password Management Policy of ICBC (Europe) S.A.
- Anti Internal Fraud Policy

1.3.2 Management of information systems and licenses of the software in use

This risky activity concerns activities related to:

- check and authorize parameter maintenance;
- Installation of software;
- make copies of software, for back-up or security purposes.

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 Cod

By way of example, 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- ICBC (Europe) S.A. Rules of IT General Management
- Information Security Policy
- ICBC (Europe) S.A.Information Technology and Information Security Incident Management Procedure
- Measures of Information and Information System Security Management

- Information System Security Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Milan Branch 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
- 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
- Anti Internal Fraud Policy

1.3.3 Use of Branch goods and services and involvement in the purchase of the same

This risky activity concerns activities related to the use of Branch assets and equipment (IT tools, information dissemination tools, equipment for duplicating texts / videos, etc.) and the involvement in the purchase of the same.

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 of damage to information, data and computer programs occurs when an employee of the Branch, abusively, enters an IT or electronic system of the Branch in order to destroy, deteriorate, delete, alter or suppress information, data or computer programs 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch Whistleblowing Policy and Procedure
- Staff Handbook
- ICBC (Europe) S.A. Rules of IT General Management
- Information Security Policy
- ICBC (Europe) S.A.Information Technology and Information Security Incident Management Procedure
- Measures of Information and Information System Security Management
- Information System Security Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Milan Branch 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
- 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
- Anti Internal Fraud Policy

1.3.4 Management of data

This risky activity concerns activities related to the data management of Branch employees and customers, with specific reference to the transmission of the data to the Headquarters (Luxembourg), Head Office (China), other Branches or to the Supervisory Authorities.

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

- Unauthorized 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)

By way of example, these offenses could occur if the employees are free to access information systems without a specific authorization, because the Branch has not adopted suitable data protection measures. In this case, from the failure to adopt the measures, the Branch could obtain a cost saving that can be configured as a profit.

In addition, consider the case of an employee of the Branch illegally accesses the customer database of a competitor in order to obtain sensitive data and to provide an unfair advantage to the Branch.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Social Media Policy
- ICBC (Europe) S.A. Rules of IT General Management
- ICBC (Europe) S.A. Rules of Privacy by Design and Privacy by Default
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A.Information Technology and Information Security Incident Management Procedure
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- Information System User Management Policy of ICBC (Europe) S.A.
- Communication Guidelines for clients
- ICBC (Europe) S.A. Data Retention Policy
- General Data Protection Regulation – Information Letter
- GDPR Privacy Notice for Recruiting
- ICBC (Europe) S.A. Milan Branch Employer Personal Data Policy
- ICBC Privacy policy
- Power of attorney Branch to HQ data transfers GDPR

- Data Transfer Agreement for ICBC (Europe) SA Milan Branch
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- Anti Internal Fraud Policy

THIRD SPECIAL PART - 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.

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 art. 24-ter of Legislative Decree 231/2001.

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.

In general, the system of organization of the Branch must respect the fundamental requirements of formalization and clarity, communication and separation of roles respecting the assigned powers.

The Branch, in order to prevent the crimes of this special part, adopts the following preventive measures:

- 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.

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

This Special Part describes the risk profiles relating to the Predicate offences included in the family of Organized Crime Offences, and therefore the crimes listed in article 24-ter of Legislative Decree 231/2001.

In relation to the aforementioned offences, the following are the Risky Activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Disbursement of loans granted by the Branch

With reference to activities related to the disbursement of loans by the Branch, the General Manager makes the final credit decision on the basis of the Credit Committee voting results.

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

listed below:

- Generic Criminal association (Article 416 of the Criminal Code)
- Mafia-type criminal association – including foreign organized crime association – and vote exchange in elections (Articles 416-bis and 416-ter)
- Criminal association for the purpose of committing the crimes relating to slavery, human trafficking and the smuggling of migrants (Article 416 of the Criminal Code, paragraphs 6 and 7)
- Association for the purpose of illicit trafficking in narcotic or psychotropic drugs (Article 74 of Presidential Decree no. 309/1990)

The intentional participation of a representative or employee of the Branch in a criminal association might of itself give rise to the entity's administrative liability, for example for criminal financing, and also could constitute an illegal practice (related to the Predicated Offence above mentioned) in financing corporations/entities with criminal managers or beneficial owners and/or have been verified or prosecuted in criminal proceedings.

Of course, must be provided that participation in or support and financing 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 organization and a common plan to carry out an indefinite series of crimes.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Internal Operation and Management Authorization
- Conflict of interest Policy
- Charter of Credit Committee
- Anti Internal Fraud Policy

FOURTH SPECIAL PART - CRIMES AGAINST INDUSTRY AND TRADE

1.1. Introduction

This Special Part 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.

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 art. 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. For identification purposes, banknote selection and acceptance equipment may

also be used, making it possible to check both the banknotes' authenticity and their suitability for circulation, or only their authenticity; alternatively, the authenticity checks can be carried out by trained staff, by means of manual checks without using selection and acceptance devices;

- must, where they detect banknotes which they suspect of being counterfeit, promptly prepare a report of withdrawal from circulation of such suspicious banknotes and report the finding to the competent Authority (Central Means of Payment Antifraud Office - UCAMP, Bank of Italy) in accordance with the procedures and time limit set out in the internal regulation;
- must hold the banknotes suspected of being counterfeit and for which the specific report was prepared in appropriate safes for the period between the date of detection/withdrawal of the banknote from circulation up to its forwarding to the Bank of Italy;
- must immediately report to their superior any attempt to circulate banknotes or valuables suspected of being counterfeit on the part of customers or third parties and of which the staff was the target or simply became aware of.

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

This Special Part describes the risk profiles relating to the Predicate offences included in the family of crimes against industry and trade, and therefore all the crimes listed in article 25-bis 1 of Legislative Decree 231/2001.

In relation to the aforementioned offences, the following are the Risky Activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Marketing of banking / financial products

In case of other new credit business, the Branch shall obtain the consent from ICBC (Europe) S.A. headquarters in Luxembourg prior to launching business.

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

- Making or possessing watermarks or instruments for the purpose of counterfeiting money, official stamps or of watermark paper (Article 461 of the Criminal Code)
- Counterfeiting, alteration or use of distinctive marks of intellectual works or industrial products (Article 473 of the Criminal Code)
- Infringement of the freedom of commerce or industry (Article 513 of the Criminal Code)
- Fraud against national Industries (Article 514 of the Criminal Code)

By way of example, the Branch could facilitate, independently or in competition with third parties and in the specific interest of the Branch, credit granting activities to entities or authors of offenses of use of counterfeit stamps, forgery of coins, etc. in the awareness of existence of illicit activities.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Banking business manual
- Charter of Credit Committee
- Anti Internal Fraud Policy

FIFTH SPECIAL PART - 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.

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.

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 financial statements 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 Bank of Italy.

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.
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.
Because of potential conflicts with the Branch, it is required that all employee obtain written approval before they accept a position as a director of a non-profit company or a position as a director, officer, employee or agent of, or consultant or advisor to, any competitor of or vendor to the Branch.
In general, all conflicts of interest, also potential, must be communicate 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 notify customers of situations of conflict of interest if the measures adopted by the Branch are not able to guarantee that the customer will not incur any damage as a result of this circumstance.

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

This Special Part describes the risk profiles relating to the Predicate offences included in the family of corporate offences, and therefore all the crimes listed in article 25-ter of Legislative Decree 231/2001.
In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Management of conflict of interests

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.
As a part of the standard control procedures the Banking Department or other relevant department review regularly the activities on accounts identified with potential conflict of interest and escalate to Legal & Compliance Department the accounts that could potentially be linked to a conflict of interest.
This activity regarding the management of the relevant information needs to identifying conflicts of interest is collected by any department of the Branch and communicated to the Legal &

Compliance Department.

The Legal & Compliance Department shall assist in the identification and monitoring of conflicts of interest and is available to provide advice to the business in that respect.

The Legal & Compliance Department will record all conflict of interests if made aware.

If any employee of Corporate & Investment Banking Department (hereafter called CIB Department) has been involved in any possible conflict of interest event (as defined in the relevant Conflicts of Interest Policy), the employee could not play any role in CIB Department of the Branch in any process related with such an event, and should comply with all the necessary procedures of Conflicts of Interest Policy of the Branch. Any potential Conflicts of Interest have to be disclosed in respect of the Conflicts of Interest 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Conflict of interest policy

- Gift Policy
- Anti Internal Fraud Policy

1.3.2 Management of the credit rating

The Branch shall assess the credit rating of customers in accordance with the measures on customers' credit rating issued by ICBC Limited (Shareholder) and ICBC (Europe) S.A. headquarters in Luxembourg and the General Manager of the Branch may approve the credit rating by maintaining or adjusting downwardly the model rating outcomes.

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)
- 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, the offence of false corporate reporting occurs when the persons in charge of the auditing process make false statements or conceal information on the profit and loss, balance sheet or cash flow situation of the audited company, in order to obtain an unfair gain for themselves or others, with full awareness of the falsity of the statements and with the intention of deceiving the recipients of the communications.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Gift Policy
- Anti Internal Fraud Policy

1.3.3 KYC and credit assessment

General Management has important tasks regarding credit risk assessment and the risks related to KYC. In particular, at GM Department are attributed, among others, powers of:

- reception and approval of the KYC plan prepared by each department
- final approval for assessment of customer credit rating
- approval for High risk clients and their eventual downgrade
- authorizes the blocking of the account of a company in the process of incorporation, in case it is not possible to carry out the identification and verification of the company's identity
- last signature to loan rescheduling on credit business

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 could be configured in the event that a client company offers money to the Branch employee in order to ensure a rescheduling of the loan.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Gift Policy
- Anti Internal Fraud Policy

1.3.4 Operating expense management

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 20.000€ are approved by the Financial 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Gift policy
- Anti Internal Fraud Policy

1.3.5 Employee management

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 Headquarters.

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 for overtime, beyond what is permitted by the Branch

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.

- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- ICBC (Europe) S.A. Milan Branch Annual Operation and Management Authorization
- Gift policy
- Anti Internal Fraud Policy
-

1.3.6 Payments and reimbursements

This risky activity concerns activities related to payments and reimbursements of welfare funds, reviewing the rationality and compliance of expenditure for welfare funds.

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)
- 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 Head of General Administration Department may review the rationality of expenditure for welfare funds for a higher amount, not in compliance with the effective cost, in order to create "black funds" for corruption purposes

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure

- Staff Handbook
- Implementation Rules for Operating Expense Management
- Conflict of interest Policy
- Gift Policy
- Anti Internal Fraud Policy

1.3.7 Trade finance business

The Banking Department and Financial Institutions Department are responsible for the operations of Trade finance, including: import and export letter of credit, inward/outward collection, T/T, import and export discounting, forfeiting, factoring, re-financing, export invoice financing, advance financing, guarantee, etc (excluding the document management activity of Trade Finance transactions that is an outsourced activity to the Headquarter).

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)
- False corporate reporting (Article 2621 of the Civil Code) Transactions prejudicial to creditors (Article 2629 of the Civil Code)
- Illegal influence on the meetings (Article 2636 of the Civil Code)

By way of example, the crime of bribery among private individuals could occur if an employee of the Branch accepts an undue money amount from a client company, in order to guarantee the Trade finance transactions even without the appropriate documents

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- Credit Management Manual
- Anti Internal Fraud Policy

1.3.8 Transaction and payment monitoring

Before executing any transaction (e.g. outward payment required by a customer, acceptance of a remittance received by a customer), the Banking Department is requested to perform a qualitative check on the requested transaction (with the cooperation of CIB Department, if necessary or advisable) to assess the integrity/accuracy/rationality of the requested transaction. Such analysis should made taking into consideration, among others, the contents of the Memo.

Following the assessment, the relevant relationship manager might request to the customer supportive documentation and/or explanation on the requested transaction as a condition for its execution.

In addition, for each inward and outward payment transactions exceeding Euro 100,000 to be made by customers holding a bank account with the Branch, the Banking Department shall mandatorily get the written approval from a Head of Legal & Compliance Department on the relevant transfer voucher before executing such transaction.

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 conduct of Senior persons in charge of preparing a Branch's financial reports, statutory auditors, liquidators and other individuals vested with powers of management within the Branch and persons under their management or supervision, who either directly or through another person, solicit or receive pecuniary benefits or other improperly provided presents and gifts or accept the promise thereof, in order to perform an act contrary to their official duties or obligations of loyalty.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- Credit Management Manual

- Gift Policy
- Anti Internal Fraud Policy

1.3.9 Account management

The Banking Department performs the account management for customers and is in charge about activities related to:

- Customer account profile management;
- Account opening/closure;
- Authorization about reactivation of dormant accounts and authorization about deviation from the standard fees;
- Check about any customer information amendment;
- Operation of the RMA exchange operation with the correspondent bank;
- Review regularly the activities on accounts identified with potential conflict of interest;
- Assist Financial Institution Department to solve detailed and technically problems while using account or other products.

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 could occur in the event that a customer offers money or other benefits to an employee of the branch so that he doesn't report activities/ transactions carried out on accounts subjected to 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Credit Management Manual
- Gift Policy
- Anti Internal Fraud Policy

1.3.10 Reporting

This risky activity concerns activities related to make spot or periodical business reporting to senior management:

- to ensure the department management is transparent with any positive and negative issue;
- for the relationships with Legal & Compliance Department for any compliance or AML related issue, as well as the potential solutions;
- for any operational risk or other risks related issue as well as the potential solutions.

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)
- Failure to disclose conflicts of interest (Article 2629-bis of the Civil Code)
- Obstruction of the duties of the Public Supervisory Authorities (Article 2638 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, the crime of bribery among private individuals could occur in the event that money is offered to an employee of the Branch so that, during the drafting of business reports, are not indicated certain problems related to transparency or the operational risk related to the customer.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Gift Policy
- Anti Internal Fraud Policy

1.3.11 Relations with Financial Intermediaries

This risky activity concerns activities related to:

- management of transactions with local and foreign Financial Institutions (e.g. insurance companies, mutual funds, security companies)

- management of the different types of relationships with the Financial Intermediaries
- prepare, organize and execute the marketing plan and actions on local financing institutions
- monitor the situation of local correspondent banks.

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.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Complaint handling Policy & procedure
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- Gift Policy
- Anti Internal Fraud Policy

1.3.12 Customers' account management and periodic monitoring

This risky activity concerns activities related to:

- customer's account opening and closing;
- customer account information modification;
- dormant customers, dormant accounts and reactivation;
- correspondence filing between the clients and the Branch;
- conduct a unified management and monitoring procedure of customer credit risks;
- analyze the documents, stamps, name check on parties involved, internet search, verify missing/ outdated documents, ensure that the input in the system is accurate, complete

missing fields, update and precise the existing input, scan the documents, complete, date and sign the reviewed check list.

All Credit facilities must be reviewed on a periodically basis according to the post-lending management measure of the Branch. CIB Department will prepare the list of credits due for review and to follow up with the Risk Management to ensure the credit facilities are reviewed on time.

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

- False corporate communications (Articles 2621 and 2621 bis of the Civil Code)
- False statements in prospectuses (Article 173-bis of Legislative Decree no. 58/1998)
- Failure to disclose conflicts of interest (Article 2629-bis of the Civil Code)
- Obstructing the activities of public regulatory authorities (Article 2638, Sections 1 and 2, of the Civil Code)
- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Unlawfully influencing the shareholders' meeting (Article 2636 of the Civil Code)
- Incitement to bribery between private parties (Article 2635 of the Civil Code)

By way of example, the offences of false corporate communications are committed by conduct which, with reference to the view of the profit and loss, balance sheet or cash flow/ credit situation of the Branch, consist in presentation of untrue material facts in the financial statements, reports or other corporate disclosures addressed to the shareholders or the general public; or omission of relevant material facts whose disclosure is required by the law.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Corporate & Investment Banking Department business manual
- Credit Management Manual
- Business Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML Policy
- Gift Policy

- Anti Internal Fraud Policy

1.3.13 Developing marketing and sales strategies

This risky activity concerns activities related to:

- promote the branch's image to Italian market;
- Develop the marketing and sales strategies with a focus on growing the business volumes and customer base;
- Management of the relationship with prospective Corporate customers and any other type of counterparties;
- Arrange meeting with potential customers;
- Represents and promotes the branch's image to niche market and local banking community.

In particular, Marketing and Credit Management functions are separately performed by CIB Department and Risk Management Department respectively. The CIB Department is the Front Office and the Risk Management Department is the Middle Office. The Marketing and Credit Management roles are performed independently by separate individuals to avoid potential conflicts of interest and to gain a fair and objective view on the risks that the Branch is undertaking.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Gift Policy

- Anti Internal Fraud Policy

1.3.14 Credit Management

This risky activity concerns activities related to:

- perform due diligence process for loans, trade finance, guarantee, etc.;
- prepare credit proposals and submit to Risk Management Department for review;
- prepare periodic review reports of performing loans; give suggestions for loan classifications and provisions;
- responsible for the fulfillment of conditions precedent before drawdown;
- perform valuation process of collaterals;
- give suggestions on the valuation result; Monitor the value of collaterals;
- monitor credit risk at customer or transaction level;
- file the credit documents and forward them to credit archives keeping department.

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

- False corporate communications (Articles 2621 and 2621 bis of the Civil Code)
- False statements in prospectuses (Article 173-bis of Legislative Decree no. 58/1998)
- Failure to disclose conflicts of interest (Article 2629-bis of the Civil Code)
- Obstructing the activities of public regulatory authorities (Article 2638, Sections 1 and 2, of the Civil Code)
- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Unlawfully influencing the shareholders' meeting (Article 2636 of the Civil Code)
- Incitement to bribery between private parties (Article 2635 of the Civil Code)

By way of example, the offence related to false statements in prospectuses could occur when any person includes false information or conceals data or news in the prospectuses required for public offerings or for admission to trading on regulated markets, or in the documents required for public purchase or exchange offers.

For this conduct to constitute an offence, the person engaging in it must act with the intention of deceiving the recipients of the prospectuses, in order to obtain an unfair profit for himself or others.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure

- Staff Handbook
- Conflict of interest Policy
- Corporate & Investment Banking Department business manual
- Credit Management Manual
- Complaint handling Policy & procedure
- AML & CTF – KYC Guidelines for the Milan Branch
- AML Policy
- Gift Policy
- Anti Internal Fraud Policy

1.3.15 Credit rating process

The credit report is submitted by the relationship manager, checked by the head of CIB Department. The credit rating process requirements are the following:

- the credit application material must be submitted for approval at least 5 working days before the facility activation;
- credit application shall be prepared by the customer's relationship manager after careful due diligence, and shall include opinions of Corporate & Investment Banking Department Head or Deputy Head;
- review of the credit application must be duly and independently performed by Head of Risk Management Department. With respect to single customer credit business, Head of Risk Management Department in principle should complete examine and give risk recommendations within 3 working days;
- single credit business within the Branch' authorization shall be discussed for collective deliberation by the Branch's credit committee and reported to the Branch's General Manager for final decision;
- when a proposed credit related business exceeds the lending authority of the Branch, after General Manager authorization, the credit application must be submitted to Credit Approval Department for review and approval.

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

- False corporate communications (Articles 2621 and 2621 bis of the Civil Code)
- False statements in prospectuses (Article 173-bis of Legislative Decree no. 58/1998)
- Failure to disclose conflicts of interest (Article 2629-bis of the Civil Code)
- Obstructing the activities of public regulatory authorities (Article 2638, Sections 1 and 2, of the Civil Code)
- Bribery among private individuals (Article 2635, paragraphs 1 and 3, of the Civil Code)
- Unlawfully influencing the shareholders' meeting (Article 2636 of the Civil Code)
- Incitement to bribery between private parties (Article 2635 of the Civil Code)

By way of example, this kind of offense takes place when the Senior person 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.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Corporate & Investment Banking Department business manual
- Charter of Credit Committee
- AML Policy
- AML & CTF – KYC Guidelines for the Milan Branch
- Gift Policy
- Anti Internal Fraud Policy

1.3.16 Accounting

This risky activity concerns activities related to:

- establish and amend the overall accounting policy and to complete and update the accounting manual;
- organizing controlling and performing the accounting treatment of the Branch;
- managing financial budget and annual assessment;
- evaluation and management, assisting to complete the annual audit.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Implementation Rules for Operating Expense Management
- Anti Internal Fraud Policy

1.3.17 Reliability and integrity of accounting and management information

This risky activity concerns activities related to the costs reporting and the collection of accounting data, the preparation and the drafting of the reports concerning accounting data to certify its completeness and truthfulness.

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)

- 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 false communications could verify when the false reporting concerns unlisted companies or those deemed equivalent thereto the presentation of untrue material facts constitutes the offence in question, only if it is contained in corporate communications required by law and if the facts are relevant.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Gift Policy
- Anti Internal Fraud Policy

1.3.18 Management of requests related to data processing

The Financial Accounting & IT Department is in charge of handling data protection requests (GDPR) as Data Protection Coordinator, cooperating with the local DPO and the DPO appointed in HQ.

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 regarding the processing of data.

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

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.

- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- ICBC Privacy policy
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- Social Media Policy
- ICBC (Europe) S.A. Rules of IT General Management
- ICBC (Europe) S.A. Rules of Privacy by Design and Privacy by Default
- ICBC (Europe) S.A. Rules of Data Lifecycle Management
- ICBC (Europe) S.A.Information Technology and Information Security Incident Management Procedure
- Information System User Management Policy of ICBC (Europe) S.A.
- Communication Guidelines for clients
- ICBC (Europe) S.A. Data Retention Policy
- General Data Protection Regulation – Information Letter
- GDPR Privacy Notice for Recruiting
- ICBC (Europe) S.A. Milan Branch Employer Personal Data Policy
- Power of attorney Branch to HQ data transfers GDPR
- Data Transfer Agreement for ICBC (Europe) SA Milan Branch
- ICBC (Europe) S.A. Milan Branch IT System Manual
- ICBC (Europe) S.A. IT Monitoring and Investigation Policy
- Gift Policy
- Anti Internal Fraud Policy

1.3.19 Second level checks and controls

Legal & Compliance Department carries out activities related to:

- carry out second level checks and controls within the Branch;
- measure and assess the non-conformity risk for the Branch, identifying and proposing any necessary remedial actions to mitigate and/or prevent any risk;
- conduct and coordinate any necessary investigation /control, check and investigations related to the Legal and AML Compliance matters.

In addition, the Risk Management Department of the Branch carries out activities related to:

- organize the Department's work to fulfil comprehensive risk management tasks with respect to identifying, measuring, analyzing, monitoring and reporting of credit risk, liquidity risk, market risk, operational risk and country risk;
- verify the periodic review report sent by Corporate & Investment Banking Department;
- verify / evaluate CIB Departments suggestions for loan classifications and provisions;

- prepare credit risk reports according to the requirements of Senior Management and ICBC Europe.

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 "Obstruction of the duties of the Public Supervisory Authorities" could potentially be configured in the case 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.

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

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Implementation Rules for Operating Expense Management
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Charter of Credit Committee
- Charter of Risk Management Committee
- AML & CTF – KYC Guidelines for the Milan Branch
- AML Policy
- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- Anti Internal Fraud Policy

1.3.20 Third level checks and controls

The Internal Audit function of ICBC (Europe) S.A. Milan Branch is located to the Headquarters in Luxembourg, and carries out the annually the following activities as part of third-level checks and controls:

- controls the regular performance of operations and the trend of risks;
- identifies anomalous trends, violations of procedures and regulations;
- evaluates the completeness, adequacy, functionality and reliability of the organizational structure and other components of the internal control system;
- brings to the attention of the corporate bodies the possible improvements to the risk management policies and any critical issues or violations found;
- based on the results of its checks, formulates recommendations to the corporate bodies.

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

- Obstruction of the duties of the Public Supervisory Authorities (Article 2638 of the Civil Code)

By way of example, the crime of obstruction of the duties of the Public Supervisory Authorities could potentially be configured in the case 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.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and procedure
- Internal Audit Charter of ICBC Europe S.A.
- Outsourcing Management Measures of ICBC (Europe) S.A. Milan Branch
- Anti-Internal Fraud Policy

1.3.22 Customer complaints management

This risky activity concerns activities related to handle the customer complaints in a timely and

sound fashion and to provide the necessary internal and external 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, 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Complaint handling Policy & procedure
- Anti Internal Fraud Policy

1.3.21 KYC and transaction monitoring

Legal & Compliance Department must exercise due diligence and Know Your Customer (hereafter called KYC) before accepting clients and/or opening a contractual relationship.

These activities are related to:

- AML/ Compliance training, watchlist screening, KYC customer due diligence reviews (including CRS and FATCA), control and approve the AML risk profile of the customer;
- AML/ Transaction monitoring; supporting and guiding the KYC unit controls and investigations in order to propose the appropriate solutions to close the alerts;
- AML/ Compliance internal reporting (including formal checks on the potential existing tax anomaly scheme and/or “reportable transaction” event in compliance with DAC-6 reporting obligation as detected by the first level controls), regulatory changes, controls, monitory and reviews.

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)
- False corporate reporting (Articles 2621 and 2621 bis of the Civil Code)
- Fictitious capital formation (Article 2632 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)
- 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 could occur if a new counterpart offers money or benefits in order to convince the Branch's employee not to report the presence of his name on the Blacklists.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- AML & CTF – KYC Guidelines for the Milan Branch
- AML Policy
- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- Gift Policy
- Anti Internal Fraud Policy

1.3.22 Management of the corporate reporting

The Risk Management Department informs the HQ periodically for the events regarding the regulatory risk indicators (capital adequacy, liquidity coverage ratio, economic capital, etc.), the quality of credit activities, the exposure to market risk and the indicators of operational risk.

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)
- 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 false corporate reporting could potentially occur in the case of communications required by law to the supervisory authorities, where facts that do not correspond to the truth are presented, even though subject to assessment, on the economic, asset or financial situation of those subject to supervision or conceal with other fraudulent means, in whole or in part, facts that should have communicated concerning the situation.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Charter of Credit Committee
- Charter of Risk Management Committee
- Gift Policy
- Anti Internal Fraud Policy

1.3.23 Reporting to Supervisory Authorities

The Internal Audit function of ICBC (Europe) S.A. Milan Branch is involved in relations and reporting of activities / documentation to Italian and Luxembourg Supervisory Authorities (i.e. Bank of Italy, Commission de Surveillance du Secteur Financier, etc), only if specifically requested. In particular the Department must comply with the current legislation and the principles of transparency, correctness, objectivity and traceability in handling relations with the Supervisory Authorities.

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 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of Interest Policy
- Suspicious Transaction Reporting Procedure
- Policy on the Manage of External Inspections
- Notice on Regulating Management of CSSF Correspondence
- Anti Internal Fraud Policy

1.3.24 Management of relations with the Supervisory Authorities

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, requests and inspections.

The contents of this 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 European Central Bank
- the Bank of Italy
- Consob
- Data Protection 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Policy on the manage of external inspections
- Gift Policy
- Suspicious transaction reporting procedure
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- Anti Internal Fraud Policy

1.3.25 Management of litigation and out-of court settlements

This risky activity concerns activities relating to:

- Review the conflict management arrangements and compliance with such by respective business areas;
- Management of attendance, absences and late arrivals of employees;
- Relationships between employees and solutions to possible conflicts.

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 offense related to corruption could occur if an employee of the Branch promises or delivers some money or other benefits towards a customer involved in a complaint, in order to dissuade him from proceeding judicially towards the Branch.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook (1.Corporate culture, 2.Terms and conditions of employment, 3. Policies, 4.Conduct and ethics)
- Conflict of interest Policy
- Anti Internal Fraud Policy

SIXTH SPECIAL PART - 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[21], 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.

[21] International Convention for the Suppression of the Financing of Terrorism signed in New York on 9.12.1999

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 Special Part 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

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.

Consequently, the Branch:

- operates so as to avoid any implication in suitable operations, even potentially, to favor the aforementioned crimes;
- refrains from executing operations for which the beneficial owner has not been adequately

identified.

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

This Special Part describes the risk relating to the Predicate offences included in the family of crimes for the purposes of terrorism or subversion of the democratic order, and therefore all the crimes listed in article 25-quater of Legislative Decree 231/2001.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Customers' relationship management and periodic monitoring

This risky activity concerns activities related to:

- customer's relationship opening and closing (ongoing relationship as qualified in compliance with AML provisions);
- customer account and updating of information and/or changes made;
- dormant customers, dormant accounts and reactivation;
- correspondence filing between the clients and the Branch;
- conduct a unified management and monitoring procedure of customer credit risks;
- analyze the documents, stamps, name check on parties involved, internet search (on qualifiable and reliable sources), verify missing/ outdated documents (evaluating the stop of transactions in case of missing AML data), ensure that the input in the system is accurate, complete missing fields, update and precise the existing input, scan the documents, complete and/or update of the AML data as required by Bank of Italy provisions on the AML storage obligation, date and sign the reviewed check list.

In addition, the General Manager has important tasks regarding the risks related to KYC. To the General Manager is attributed, among others, powers of:

- reception and approval of the KYC plan prepared by each department;
- final approval for High risk clients after Client and Relationship Acceptance Committee proposal;
- authorizes the blocking of the account of a company in the process of incorporation, in case it is not possible to carry out the identification and verification of the company's identity;
- last signature to loan rescheduling on credit business.

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)
- Participation in financing the enemy (Article 249 of the Criminal Code) 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Banking business manual
- Corporate & Investment Banking Department business manual
- Suspicious Transaction Reporting Procedure
- Business Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML Policy
- Anti Internal Fraud Policy

1.3.2 KYC and transaction monitoring

The Legal & Compliance Department must exercise due diligence and Know Your Customer (hereafter called “KYC”) before accepting borrowers or clients. These activities are related to:

- AML / Compliance training, watchlist screening, KYC customer due diligence reviews (including CRS and FATCA), control and approve the AML risk profile of the customer;

- Monitoring of the correct execution of AML and CTF checks on designated terrorists and about the compliance with the international restrictive measures (included embargoes and international, and EU and national sanctions too)
- AML / Transaction monitoring, supporting and guiding the KYC unit controls and investigations in order to propose the appropriate solutions to close the alerts;
- AML / Compliance internal reporting, regulatory changes, controls, monitory and reviews.
- Handle the customer complaints in a timely and sound fashion and to provide the necessary internal and external reporting.

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

- Financing terrorist activities (art. 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies" art. 270-quinquies 2 code of civil procedure)
- Participation in financing the enemy (Article 249 of the Criminal Code) 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 (and entities) 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 embargo or other operational restrictions, or with subjects that carry out suspected activities at risk of money laundering.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- AML & CTF – KYC Guidelines for the Milan Branch

- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML Policy
- Anti Internal Fraud Policy

1.3.3 KYC and credit assessment

General Management has important tasks regarding credit risk assessment and the risks related to KYC. In particular, at General Management are attributed, among others, powers of:

- reception and approval of the KYC plan prepared by each department;
- final approval for assessment of customer credit rating;
- approval for High risk clients and their eventual downgrade;
- authorizes the blocking of the account of a company in the process of incorporation, in case it is not possible to carry out the identification and verification of the company's identity;
- last signature to loan rescheduling on credit business.

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

- Financing terrorist activities (art. 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies" art. 270-quinquies 2 code of civil procedure)
- Participation in financing the enemy (Article 249 of the Criminal Code) 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 of financing terrorism activities could arise in the case that GM approves the granting of a credit to a client who, according to KYC's plan, is highly at risk of involvement in terrorist associations, for the sole purposes of expanding the Branch's business.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook

- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.4 Transaction and payment monitoring

Before executing any transaction (e.g. outward payment required by a customer, acceptance of a remittance received by a customer), the Banking Department is requested to perform a qualitative check on the requested transaction (with the cooperation of CIB Department, if necessary or advisable) to assess the integrity/accuracy/rationality of the requested transaction. Such analysis should made taking into consideration, among others, the contents of the Memo. Following the assessment, the relevant relationship manager might request to the customer supportive documentation and/or explanation on the requested transaction as a condition for its execution. In addition, for each inward and outward payment transactions exceeding Euro 100,000 to be made by customers holding a bank account with the Branch, the Banking Department shall mandatorily get the written approval from a compliance officer on the relevant transfer voucher before executing such transaction.

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

- Financing terrorist activities (art. 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies" art. 270-quinquies 2 code of civil procedure)
- Participation in financing the enemy (Article 249 of the Criminal Code) 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 offence could occur if the Branch authorizes a transaction despite the risk arising from the fact that names of the subjects involved in the transactions are included in the lists provided by the Authorities of Public Security, or by Bank of Italy and the FIU because they are suspected of and/or involved in terrorism conducts and/or financing 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Anti Internal Fraud Policy

1.3.5 **AML/CTF Due Diligence and Client Onboarding Procedure**

The Corporate and Investment Banking Department and the Financial Institutions Department carry out significant activities related to the acceptance procedure of the counterpart, the due diligence process of anti-money laundering and counter-terrorism financing through activities such as, among others:

- collect and review archive about KYC documentation collection process and AML risk assessment;
- Report in the case of suspicious behaviors and / or transactions;
- Monitoring of the counterpart relationship;
- perform the appropriate controls.

In the customer's relationship context it is mandatory the acquiring of all data, information, including those having tax connection, referred to all delegates having or to whom have been granted powers to operate into the relationship, including the acquiring of the ultimate beneficial owners, in order to fulfill the customer's due diligence obligation and the tax reporting obligations.

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

- Financing terrorist activities (art. 270-quinquies 1 code of civil procedure)
- Embezzlement of confiscated assets or monies" art. 270-quinquies 2 code of civil

procedure)

- Participation in financing the enemy (Article 249 of the Criminal Code) 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 of financing terrorist activities could occur if the employee of the Branch in charge of reporting suspicious transactions/conduct omits the report, despite the risk that the counterparty is involved in terrorist associations and/or is included in international, UE and/or local restrictive lists.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML & CTF – KYC Guidelines for the Milan Branch
- Anti Internal Fraud Policy

SEVENTH SPECIAL PART - 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 Special Part, 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 Special Part 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.

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 follow 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 Headquarters for approval before the hired. The annual scope of authority shall be determined by Headquarters 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

This Special Part describes the risk relating to the Predicate offences included in the family of crimes against individual, and therefore all the crimes listed in article 25- quinquies of Legislative Decree no.231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Management of the staff selection and recruitment process

This risky activity concerns activities related to:

- planning, updating and management of recruiting processes;
- performance monitoring during probationary period, coordination the training of staff;
- elaboration of the request of employees to carry out external business activities and review the conflict management arrangements and compliance with such by respective business areas;
- relationships between employees and solutions to possible conflicts;
- health and safety and workplace risks, in accordance with the contents of Legislative Decree no. 81/2008.

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:

- 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch

- Whistleblowing Policy and Procedure
- Staff Handbook
- The Administrative Measures for Staff Recruitment of ICBC(Europe) S.A Milan Branch
- Conflict of interest Policy
- Anti Internal Fraud Policy

EIGHTH SPECIAL PART - 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. 58/1998 [22] (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 on behalf of the Branch or in favor of Branch customers where the Branch itself is also set to gain from such acts, and dissemination of false or

[22] Law no. 62/2005 introduced in Articles 184 and 185 of Legislative Decree no. 58/1998 (Consolidated Law on Financial Intermediation, hereinafter the "Consolidated Law on Finance"), the offences of "insider trading" and of "market manipulation", as well as two corresponding types of administrative offence, set out in Articles 187-bis and 187-ter of the Consolidated Law on Finance.

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; the Bank might also in theory become involved in the offence committed by the customer having regard to the concrete manner of performance of the Bank’s activity.

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, Internal Audit, Risk Management. 'Restricted information' may only be passed between business areas in accordance with the 'need to know' principle and the cross separation procedure.

The Branch prohibits of its employees trading in the securities of any company while in possession of material, non-public information regarding the company.

If the Employee has into possession of insider information, they may not execute any trade in the securities of the subject company without first consulting with the Head of Legal & Compliance Department. The Head of Legal & Compliance Department will determine whether such trade violate the branch’s policy and hence, potential subject to the prohibition on insider training. In particular, if there is a substantial likelihood that a reasonable investor considers the information important in determining whether to trade in a security, or if the information, if made public likely would affect the market price of a company’s securities.

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 “nonpublic” 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 a sufficient number of suspicious orders or transactions to accumulate reporting.

Lastly, the Branch has adopted rules regarding market dealing in order to sets out specific rules of conduct based on the legal reporting requirements for transactions performed on the financial instruments of a listed issuer by relevant and/or related parties, for the purpose of ensuring that the information provided to the market meets the highest standards of transparency.

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

This Special Part describes the risk relating to the Predicate offences included in the family of Market abuse, and therefore all the crimes listed in article 25-sexies of Legislative Decree no. 231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Management of the restricted information

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, Internal Audit, Risk Management. 'Restricted information' may only be passed between business areas in accordance with the 'need to know' principle and the cross separation procedure.

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. 'Restricted information' may only be passed between business areas in accordance with the 'need to know' principle and the cross separation procedure.

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 such 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 certain of the transactions referred to above.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Credit Management Manual
- Charter of Credit Committee
- Conflict of interest Policy
- Implementing Regulations on Financial Market Business Verification
- Anti Internal Fraud Policy

1.3.2 KYC and credit assessment

General Management has important tasks regarding credit risk assessment and the risks related to KYC. In particular, at General Management are attributed, among others, powers of:

- reception and approval of the KYC plan prepared by each department;
- final approval for assessment of customer credit rating;
- approval for High risk clients and their eventual downgrade;
- authorizes the blocking of the account of a company in the process of incorporation, in case it is not possible to carry out the identification and verification of the company's identity;
- last signature to loan rescheduling on credit business.

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 training could occur considering that the General Management of the Branch is in possession of privileged information regarding the client companies and could exploit them to carry out transactions on the stock exchange, personally or through third parties, deriving undue economic advantages.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.3 Relations and information flows with Headquarters

The General Manager is in charge to report, if required, any business decision or information to the Headquarters in Luxemburg. For example, in the event, that companies for record business are subject to a loan restructuring. The General Management must report the information to ICBC (Europe) S.A. Headquarters in Luxembourg for record.

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 the 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.4 Relations with Financial Intermediaries

This risk activity concerns activities related to:

- management of transactions with local and foreign Financial Institutions (e.g. insurance companies, mutual funds, security companies);
- management of the different types of relationships with the Financial Intermediaries;
- prepare, organize and execute the marketing plan and actions on local financing institutions;
- monitor the situation of local correspondent banks.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Implementation Rules for Operating Expense Management
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- Anti Internal Fraud Policy

1.3.5 Credit rating process

The credit report is submitted by the relationship manager, checked by the head of CIB Department.

The credit rating process requirements are the following:

- the credit application material must be submitted for approval at least 5 working days before the facility activation;
- credit application shall be prepared by the customer's relationship manager after careful due diligence, and shall include opinions of Corporate & Investment Banking Department Head or Deputy Head;
- review of the credit application must be duly and independently performed by Head of Risk Management Department. With respect to single customer credit business, Head of Risk Management Department in principle should complete examine and give risk recommendations within 3 working days;
- single credit business (except low-risk business) within the Branch' authorization shall be discussed for collective deliberation by the Branch's credit committee and reported to the Branch's General Manager for final decision;
- when a proposed credit related business exceeds the lending authority of the Branch, after General Manager authorization, the credit application must be submitted to Approval Center for review and approval.

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 offense could occur if an employee of the Branch uses illegally the information acquired during the preliminary phase connected with the credit rating, in order to carry out operations (purchase, sale, recommendation to others to operate, etc.) on listed financial instruments for the benefit of the institution itself.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Corporate & Investment Banking Department business manual
- Charter of Credit Committee
- AML Policy
- AML & CTF – KYC Guidelines for the Milan Branch
- Anti Internal Fraud Policy

1.3.6 Internal dealing regarding privileged information acquired through the credit process

This risky activity concerns activities related to the potential acquisition and utilization of privileged information regarding business choices of corporate clients of the Branch, during the preliminary investigation phase and acquisition of customer information for the request for funding.

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 abuse of insider information is abstractly characterized by the diffusion of precise information, not previously made public, 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Corporate & Investment Banking Department business manual
- Charter of Credit Committee
- AML Policy
- AML & CTF – KYC Guidelines for the Milan Branch
- Anti Internal Fraud Policy

1.3.7 Management of the corporate reporting

The Risk Management Department informs the HQ periodically for the events regarding the regulatory risk indicators (capital adequacy, liquidity coverage ratio, economic capital, etc.), the quality of credit activities, the exposure to market risk and the indicators of operational risk.

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 occurs when a person buys, sells, or carries out other transactions for his own account or for the account of a third party, on financial instruments using inside information he possesses by virtue of (i) his membership of the administrative, management or supervisory bodies of the issuer or (ii) his holding in the capital of an issuer or (iii) the exercise of his employment, profession, duties, including public duties, or position.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization

- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Charter of Credit Committee
- Anti Internal Fraud Policy

NINTH SPECIAL PART - 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 Special Part 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 probably incurable condition; the loss of a sense, a limb, an organ or the capacity to procreate, permanent impairment of the power of speech, and facial deformity or permanent disfigurement.

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.

1.2. General rules of conduct

The Branch promotes a health and safety work place.

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. It will be their duty to ensure that the policy is upheld at all times and to provide the necessary funds and manpower required.

For a Health and Safety Policy to be 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 as 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 Managers, give their name, location and brief details of the problem.

All accidents must be reported to the General Managers who 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

This Special Part describes the risk relating to the Predicate offences included in the family of workplace health and safety offences, and therefore all the crimes listed in article 25-septies of Legislative Decree no. 231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Responsible for security

This activity regarding the contracts or agreements related to security business, including security project planning, security project implementation, procurement of security equipment, maintenance of security equipment, security risk assessment, security training and drill, security service outsourcing.

The General Managers of the Branch have an obligation to put in place all systems necessary to ensure the effectiveness and the concrete implementation of the control and conduct principles described in this protocol.

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

- Involuntary manslaughter (Article 589 of the Criminal Code)
- Involuntary serious or grievous bodily injury (Article 590 paragraph 3 of the Criminal Code)

By way of example, the hypothesis of crime could occur if an employee of the Branch is involved in an accident at work caused by non-compliance with the Branch premises to the rules prescribed by the law on health and safety at work (fire maintenance, electrical systems, etc).

In addition, by way of example the Predicated Offence could occur if the Branch do not take and implement all adequate measures to prevent the health of all Recipients in case of a pandemic disease.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Anti Internal Fraud Policy

TENTH SPECIAL PART - 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[23] 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

[23] Legislative Decree no. 231 of 21.11.2007 and following amendments, which transposed Community law by strengthening the Italian legislation on the prevention of the use of the financial system for the purpose of money laundering and on the fight against the financing of terrorism.

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.

1.2. General rules of conduct

As a commercial Branch that offers customers with diversified financial products and services, the

branch takes seriously its obligation to join 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 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, 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 AML/CFT officer of the Branch. The officer will decide whether reporting to competent authorities is requires.

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 mandatory 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

This Special Part describes the risk relating to the predicate crimes concerning receipt of stolen goods, money laundering and use of money, goods or benefits of unlawful origin, as well as self-laundering, and therefore all the crimes listed in article 25-octies of Legislative Decree no. 231/01.
In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Operation and Management Authorization

The approval authority of the General Manager of the Branch is specified in the Annual Internal Operation and Management Authorization granted by ICBC Europe Headquarter.
In particular, the General Manager of the Branch has the authorization for approval if the planned total amount of credit limit and the debt investment limit of a corporate customer within its credit region does not exceed the previous total amount (i.e. the latest determined or adjusted total amount), on condition that the requirements of reference credit limit management are complied with.
The credit limit for a single corporate customer out of the Branch's credit region or a group of affiliated customers shall be reported to ICBC (Europe) S.A. headquarters in Luxembourg for approval.
For the credit business "pledge of high-quality financial assets of corporate customers credit business" or "corporate credit business backed by high-quality financial institutions and sovereign entities" (except credit business against cross-border security), the Branch's General Manager's authorization is not subject to the approval rules for single credit transaction as set in the Annual Internal Operation and Management Authorization.
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 Branch could respond by way of competition in the crime of money laundering, in the case of in case of approval of loans to unidentified counterparties or in case of the final destination of the loan is not clear.
The Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by

the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.2 Monitoring of operations and dealing

The approval authority of the General Manager of the Branch is specified in the Annual Internal Operation and Management Authorization granted by ICBC Europe 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, with regard to cash deposits, which is one of the product offered by Branch to its customers, the mere acceptance by the Branch of a deposit could give rise to the “placement” and “layering” phases, that are typical of money laundering (i.e. placement of cash with the bank, with the obligation of the bank to refund and equivalent sum).

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure

- Staff Handbook
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.3 Credit Approval Authority

The Credit Committee will assist entire General Management's (hereafter called GM) credit decision.

The approval authority of GM is specified in Branch's Annual Operation and Management Authorization granted by ICBC Europe.

When the proposed credit exposure exceeds the lending authority of the GM of the Branch, the proposal will be forwarded to Head Quarter or subsequently to Head Office.

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, money laundering consists of dynamic actions aimed at putting the goods into circulation, whereas their mere receipt or concealment could give rise to the offence of receipt of stolen goods. With regard to Branch relationships, for example, the mere acceptance of a deposit could give rise to the replacement conduct which is typical of money laundering (replacement of cash with bank money, irrespective of the balance of the deposit).

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook

- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.4 AML/CTF Due Diligence and Client Onboarding Procedure

The Corporate and Investment Banking Department and the Financial Institutions Department carry out significant activities related to the acceptance procedure of the counterpart, the due diligence process of anti-money laundering and counter-terrorism financing through activities such as, among others:

- collect and review archive about KYC documentation collection process and AML risk assessment;
- Report in the case of suspicious behaviors and / or transactions;
- Monitoring of the counterpart relationships in comparison with the expected transactions as declared by the customer in the context of the due diligence process ;
- perform the appropriate controls.

In the customer's relationship context it is mandatory the acquiring of all data, information, including those having tax connection, referred to all delegates having or to whom have been granted powers to operate into the relationship, including the acquiring of the ultimate beneficial owners, in order to fulfill the customer's due diligence obligation and the tax reporting obligations.

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)
- 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)
- Instigating bribery among private individuals (art. 2635 bis, par. 1 of the Civil Code)

By way of example, the crime could be committed by (i) facilitating any omitted and/or incomplete acquiring of AML mandatory data and/or any conduct in performing a de-risking of the customer's risk classification; (ii) the making of any conducts to hinder/conceal the evaluation and/or reporting of suspicious transaction reporting; (iii) performing any action to obstruct the appropriate controls. The crime of obstacle to the exercise of the functions of the Public Supervisory Authorities could potentially occur also in the case of the realization of one of the following behaviors: 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 obstacle to the functions of the Public Supervisory Authorities, even if they omit the communications due to the Authorities (Tax Authorities too).

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML & CTF – KYC Guidelines for the Milan Branch
- Gift Policy
- Anti Internal Fraud Policy

1.3.5 KYC and transaction monitoring

Legal & Compliance Department must therefore exercise due diligence and Know Your Customer (hereafter called KYC) before accepting borrowers or clients or approving the entering into a customer's relationship.

These activities are related to:

- AML/ Compliance training, watchlist screening, KYC customer due diligence reviews (including CRS and FATCA and the risk events verification), control and approve the AML

risk profile of the customer;

- AML/ Transaction monitoring, (including formal checks on the potential existing tax anomaly scheme and/or “reportable transaction” event in compliance with DAC-6 reporting obligation and/or any illicit tax scheme or fraud as published by the local FIU and/or as detected by the first level controls) supporting and guiding the KYC unit controls and investigations in order to propose the appropriate solutions to close the alerts;
- AML/ Compliance internal reporting (including formal checks on the potential existing tax anomaly scheme and/or “reportable transaction” event in compliance with DAC-6 reporting obligation as detected by the first level controls), regulatory changes, controls, monitory and reviews.

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, for the offence to occur, the culprit needs not have acted for the purpose of obtaining some gain or of helping the perpetrators of the underlying crime to secure the proceeds of their crime. Money laundering consists of dynamic actions aimed at putting the goods into circulation, whereas their mere receipt or concealment could give rise to the offence of receipt of stolen goods.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- AML & CTF – KYC Guidelines for the Milan Branch
- Suspicious Transaction Reporting Procedure
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML Policy
- Anti Internal Fraud Policy

1.3.6 KYC and credit assessment

General Management has important tasks regarding credit risk assessment and the risks related to KYC. In particular, at GM are attributed, among others, powers of:

- reception and approval of the KYC plan prepared by each department;
- final approval for assessment of customer credit rating;
- approval for High risk clients and their eventual downgrade;
- authorizes the blocking of the account of a company in the process of incorporation, in case it is not possible to carry out the identification and verification of the company's identity;
- last signature to loan rescheduling on credit business.

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 Branch employee could be responsible for money laundering if he allows a client company to maintain his account, even though it is not possible to carry out the necessary checks on it, in order to ensure that large amounts of money pass through the accounts 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Banking Business Manual
- Anti Internal Fraud Policy

1.3.7 Operating expense management

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 20.000€ are approved by the Financial 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Anti Internal Fraud Policy

1.3.8 Trade finance business

The Banking Department and Financial Institutions Department are responsible for the operations of Trade finance, including: import and export letter of credit, inward/outward collection, T/T, import and export discounting, forfeiting, factoring, re-financing, export invoice financing, advance financing, guarantee, etc (excluding the document management activity of Trade Finance transactions that is an outsourced activity to the 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 crime of money laundering could occur if the responsible of the Banking

Department of the Branch carries out a suspected trade finance operation requested by a client, failing to send the appropriate report to the Head of Legal & Compliance Department.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Credit Management Manual
- Trade finance & settlement manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Anti Internal Fraud Policy

1.3.9 Transaction and payment monitoring

Before executing any transaction (e.g. outward payment required by a customer, acceptance of a remittance received by a customer), the Banking Department is requested to perform a qualitative check on the requested transaction (with the cooperation of CIB Department, if necessary or advisable) to assess the integrity/economic congruity/accuracy/rationality of the requested transaction. Such analysis should made taking into consideration, among others, the contents of the Memo, having specific care to Anomaly Schemes as issued by the relevant authorities – Financial intelligence Unit – (UIF) including those having tax relevance as pointed out by the November 10th communication[24]).

Following the assessment, the relevant relationship manager might request to the customer supportive documentation and/or explanation on the requested transaction as a condition for its execution.

[24] Pls refer to "Schemes representing abnormal conducts . transactions and/or activities related to tax crimes – as per L. D. 231/07 art. 6 co. 7 lett. B).

In addition, for each inward and outward payment transactions exceeding Euro 100,000 to be made by customers holding a bank account with the Branch, the Banking Department shall mandatorily get the written approval from a Head of Legal & Compliance Department on the relevant transfer voucher before executing such transaction.

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 of money laundering may be configured in the event that the employee responsible for monitoring transactions fails to report any suspicious transactions ordered by the customer or fails to carry out a qualitative control of the transaction despite being aware of the illicit operation.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Trade finance & settlement manual
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure
- Anti Internal Fraud Policy

1.3.10 Account management

The Banking Department performs the account management for customers and is in charge about activities related to:

- Customer account profile management
- Account opening/closure
- Authorization about reactivation of dormant accounts and authorization about deviation from the standard fees
- Check about any customer information amendment
- Operation of the RMA exchange operation with the correspondent bank
- Review regularly the activities on accounts identified with potential conflict of interest
- Assist Financial Institution Department. to solve detailed and technically problems while using account or other products

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 where a person, who did not aid and abet commission of the underlying crime, substitutes or transfers money, goods or other assets deriving from an intentional offence or carries out other transactions in respect of such money, goods or assets, so as to obstruct 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Banking business manual
- Credit Management Manual
- AML & CTF – KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting Procedure

- Anti Internal Fraud Policy

1.3.11 Management and collection of liquidity

This risky activity concerns activities related to:

- liquidity management in order to optimize the "Liquidity Coverage Ratio" and “Net Stable Funding Ratio” indicators;
- preparation and daily submission of an internal report on cash flows, analyzing cash flows, main sources of financing and market conditions;
- preparation of the liquidity provision plan to manage any cash imbalances.

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 kind of offense could be configured by investing directly benefiting the Branch, without using the availability on the Branch's current accounts and money from crime, in order to favor the re-entry into the legal circuit of money deriving from illicit; or inserting fictitious expenses into the Branch's management and accounting system and transferring money from illegal activity, in order to favor its re-entry into the economic circuit, and 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit institutions, Financial Institutions and Assimilated Financial Institutions
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML & CTF – KYC Guidelines for the Milan Branch
- Anti Internal Fraud Policy

1.3.12 Customer relationships

This risky Activity concerns activities related to:

- promote products and services, introduce products and services to the customer and structure the transaction;
- management of the relationship with actual Corporate customers and any other type of counterparties;
- manage and maintain existing customer relationships as well as develop new relationships.

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 crimes under consideration could occur if the person in charge of the Department facilitates the execution of operations related to money, assets or other benefits deriving from non-negligent crime, in order 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Complaint handling Policy & procedure
- Credit Management Manual
- AML Policy for the Milan Branch in the preventive measures
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- Suspicious Transaction Reporting Procedure
- AML & CTF – KYC Guidelines for the Milan Branch
- Anti Internal Fraud Policy

1.3.13 Accounting

This risky activity concerns activities related to:

- establish and amend the overall accounting policy and to complete and update the accounting manual;
- organizing controlling and performing the accounting treatment of the Branch;
- Managing financial budget and annual assessment,
- evaluation and management, assisting to complete the annual audit.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Implementation Rules for Operating Expense Management
- Anti Internal Fraud Policy

1.3.14 Management of relations with the financial administration (including Tax Authorities)

This risky activity concerns activities related to handle the local tax affairs of the Branch and the treasury back office function.

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Implementation Rules for Operating Expense Management
- AML Policy
- Anti Internal Fraud Policy

1.3.15 Verification and monitoring on accounting data

The Financial Accounting & IT Department is responsible for the accuracy and correctness of accounting records and the preparation of financial statements and statistic reports which conform to regulatory requirements and the adequate tax rules and practices.

In collaboration with the Risk Management Department conduct two levels of verification on the quality, correctness and completeness of the data of Centrale Rischi Reporting: before transmitting the data to Engineering S.p.A., the data are reconciled with the financial reports and the financial statements of the Branch. After having received the supervisory reports from the outsourcer, a check on the data is carried out with respect to the original data and the balance sheet reports in order to verify the correct and complete execution of the work.

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 kind of offense could be configured by inserting fake suppliers or customers in the management and accounting system of the Branch and transferring money from illegal activity, in order to facilitate its re-entry into the economic balance, obtaining also a monetary

advantage from carrying out this activity or an illicit tax advantage.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Anti Internal Fraud Policy

1.3.16 Appointment and relations with professional consultants

This risky activity concerns activities related to the appointment of professional consultants, in particular intellectual services including qualified consultancy activities, in order to support specific audit activities to carry out at Branch level.

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 of money laundering could be realized in the purchasing of consultancy services for non-existent services, in order to hide the real illicit origin of money or facilitate, through tax offences committing crimes, the money laundering of such illicit funds or, having the same purpose, by using the banking and financial services and/or products of the Branch to hide illicit funds.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- The Administrative Measures for Staff Recruitment of ICBC
- Whistleblowing Policy and procedure

- AML Policy
- Internal Audit Charter of ICBC Europe S.A.
- Outsourcing Management Measures of ICBC (Europe) S.A. Milan Branch
- Anti Internal Fraud Policy

1.3.17 Procurement of goods and services

This risky activity concerns activities related to the negotiation / conclusion of contracts for appointments and procurement of goods and services, the execution of works and the assignment of consulting 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, the crime of money laundering could be realized in the purchasing of consultancy services for non-existent services, in order to hide the real illicit origin of money.

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

- Code of Ethics
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Whistleblowing Policy and procedure
- Staff Handbook
- Conflict of interest Policy
- AML Policy
- Implementation Rules for Operating Expense Management
- Conflict of interest Policy
- Anti Internal Fraud Policy

ELEVENTH SPECIAL PART - 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

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 Special 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-SIAE 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

This Special Part describes the risk relating to the predicate crimes involving breach of copyright, and therefore all the crimes listed in article 25-novies of Legislative Decree no. 231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Use of Branch goods and services and involvement in the purchase of the same

This risky activity concerns activities related to the use of Branch assets and equipment (IT tools, information dissemination tools, equipment for duplicating texts / videos, etc.) and the involvement in the purchase of the same.

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, is punished the unauthorised duplication and import, 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).

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

- Code of Ethics
- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization

- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Social Media Policy
- ICBC (Europe) S.A. Rules of IT General Management
- ICBC (Europe) S.A. Rules of Privacy by Design and Privacy by Default
- Information Security Policy
- ICBC (Europe) S.A. Information Technology and Information Security Incident Management Procedure
- Measures of Information and Information System Security Management
- Information System Security Management
- ICBC (Europe) S.A. Rules of Information System Operation Management
- ICBC (Europe) S.A. Milan Branch Breach Management Procedure
- Rules of IT Resource Management
- Rules of Key Resources Security Management
- ICBC (Europe) S.A. Milan Branch IT System Manual
- Anti Internal Fraud Policy

1.3.2 Management of the credit files

The General Management oversees the activities related to:

- storage of the credit files;
- the security, access, destroying and secret keeping of the credit files.

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)
- Un-authorized 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, this offence is committed by anyone who abusively gains access to a computer system or telecommunications system protected by safety measures or retains access thereto against the will of any person who is entitled to deny such access.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Banking Business Manual
- Implementing Regulations on Credit Archives Management
- Anti Internal Fraud Policy

TWELFTH SPECIAL PART - 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 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 in connection with criminal proceedings, if such person has the right to remain silent. This crime is provided for by article 377-bis of the Criminal Code.

Moreover, pursuant to Article 10 of Law no. 146/2006 it can entail the same liability also where the offence is of transnational scope (see the Fifteenth Special Part).

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 Special 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

This Special Part describes the risk relating to the predicate crimes of inducement not to make or to make false statements to judicial authorities and therefore all the crimes listed in article 25-decies of Legislative Decree no. 231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Management of the participation to the judicial and out-of-court litigation

This protocol applies to all the Branch Structures involved in the management of judicial and out-of court litigation (administrative, civil, criminal - and criminal tax included - , tax, labor and social security litigation).

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Policy on the manage of external legal advisors
- Anti Internal Fraud Policy

THIRTEENTH SPECIAL PART - 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.

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 Special 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

This Special Part describes the risk relating to the predicate crimes of employment of third-country citizens whose stay is irregular and therefore all the crimes listed in article 25-duodecies of Legislative Decree no. 231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Management of the staff selection and recruitment process

This risky activity concerns activities related to:

- planning, updating and management of recruiting processes;
- performance monitoring during probationary period, coordination the training of staff;
- elaboration of the request of employees to carry out external business activities and review the conflict management arrangements and compliance with such by respective business areas;
- relationships between employees and solutions to possible conflicts;
- health and safety and workplace risks, in accordance with the contents of Legislative Decree no. 81/2008;
- 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:

- Employment of illegal aliens (Article 22, paragraph 12-bis, Legislative Decree no. 286/1998 – Consolidated Law on Immigration, which is mentioned in art, 25-duodecies of the Decree)

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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch

- Whistleblowing Policy and Procedure
- Staff Handbook
- The Administrative Measures for Staff Recruitment of ICBC (Europe) S.A Milan Branch Internal
- Conflict of interest Policy
- Anti Internal Fraud Policy

FOURTEENTH SPECIAL PART - 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 of the Criminal Code.

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

This Special Part describes the risk relating to the predicate crimes of racism and xenophobia and therefore all the crimes listed in article 25-terdecies of Legislative Decree no. 231/01.

In relation to the aforementioned offences, the following are the Risky activities identified within the

Branch and the main methods of implementation of the same.

1.3.1 Employee management

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 Headquarters.

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:

- 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, because of his religious, political or sexual orientation.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- The Administrative Measures for Staff Recruitment of ICBC(Europe) S.A Milan Branch Internal
- Staff Handbook
- Anti Internal Fraud Policy

1.3.2 Management of the staff selection and recruitment process

This risk activity concerns activities related to:

- planning, updating and management of recruiting processes;
- performance monitoring during probationary period, coordination the training of staff;
- elaboration of the request of employees to carry out external business activities and review the conflict management arrangements and compliance with such by respective business areas;
- relationships between employees and solutions to possible conflicts;
- health and safety and workplace risks, in accordance with the contents of Legislative Decree no. 81/2008.

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:

- Racism and xenophobia (art. 604-Bis, paragraph 3 of the criminal code)

By way of example, in this case is punished the 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 Recipients of the Model who operate in the context of this activity, in compliance with the general principles stated in the Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- The Administrative Measures for Staff Recruitment of ICBC(Europe) S.A Milan Branch Internal
- Conflict of interest Policy
- Anti Internal Fraud Policy

FIFTEENTH SPECIAL PART - TRANSNATIONAL OFFENCES

1.1. Introduction

The liability of Entities for this category of offence is laid down in Law no. 146/2006, in order to enhance the effectiveness of the fight against transnational organized crime.

An offence is considered to be transnational and is punished with a term of imprisonment of not less than four years, where it involves an organized criminal group and:

- was committed in more than one Country, or
- was committed in one Country, but a significant part of its preparation, planning, management or control took place in another Country, or
- was committed in one Country, but involved an organized criminal group which pursues criminal activities in more than one Country;

- was committed in one Country, but had significant impact in another Country.

Many of the crimes already mentioned in the previous special sections may give rise to the Entity's liability where the twofold conditions of the entity's interest or advantage and of the translational nature of the crime (of which the offender must have been aware) are met.

In particular, this Special Part includes the crimes of criminal associations under Articles 416 and 416-bis of the Criminal Code, criminal associations for the smuggling of foreign tobacco products or for trafficking in drugs of abuse, offences relating to the smuggling of migrants, inducement not to make or to make false statements to judicial authorities, aiding a fugitive.

1.2. General rules of conduct

- The Branch, in order to prevent the crimes mentioned in this special section, prepares the following risk mitigation measures. operates in such a way as to avoid any involvement in operations that are suitable, even potentially, to favor said crimes.

In any case, for the offences included in this category and therefore can take on a transnational character, are subject to the general rules of conduct set out in the previous paragraphs.

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

This Special Part describes the risk relating to the predicate crimes of transnational offences and therefore all the crimes laid down in Law no. 146/2006.

In relation to the aforementioned offences, the following are the Risky Activities identified within the Branch and the main methods of implementation of the same.

1.3.1 Activities related to the participation in the credit process

The General Management has the power of approval/credit business within the Branch's authority or Approval Center for rating upgrade and credit limit authorization and all credit related business beyond the Branch's authority.

The Corporate & Investment Banking Department has a relationship manager role with tasks such as: arrange meeting with potential customers, maintain the customer-Branch relationship, perform due diligence process for loans, prepare periodic review reports of performing loans, give suggestions for loan classification and provisions, liaise with customers to ensure all necessary documents are executed and all the conditions precedent have been fulfilled.

In addition, the Risk Management Department participates in the credit procedure during the phases of credit rating and credit limit, review of credit proposal, summary credit analysis report, periodic review, loan classification and provision.

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

- Criminal associations (Articles 416 and 416-bis of the Criminal Code)
- Criminal associations for the smuggling of foreign tobacco products (Article 291-quater of

Presidential Decree no. 43/1973)

- Criminal associations for trafficking in drugs of abuse (Article 74 of Presidential Decree no. 309/1990)
- Offences relating to the smuggling of migrants (Article 12, paragraphs 3, 3-bis, 3-ter and 5 of Legislative Decree no. 286/1998)
- Aiding a fugitive (Article 378 of the Criminal Code)

By way of example, the intentional participation of a representative or employee of the Branch in a criminal association might of itself give rise to the entity's administrative liability, for example for international criminal financing. Of course, must be provided that participation in or support and financing 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 organization and a common plan to carry out an indefinite series of crimes.

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Credit Management Manual
- Internal Operation and Management Authorization
- Charter of Credit Committee
- Anti Internal Fraud Policy

SIXTEENTH SPECIAL PART - TAX PREDICATED OFFENSES

1.1. Introduction.

Article 25-quinquiesdecies of Legislative Decree 231/01 provides for the administrative liability of the Entity in case of fiscal / tax crimes commission.

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.

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 - Headquarters - 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.

The several types of offenses are:

(1→) (art. 2 Legislative Decree no. 74/2000) "Fraudulent declaration through the use of invoices or other documents for non-existent operations".

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.

(2→) (Article 3 of Legislative Decree no. 74/2000) "Fraudulent declaration by other means".

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 through 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.

(3→) 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 declarations 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.

(4→) 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.

(5→) 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.

(6→) 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).

(7→) 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.

(8→) 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 of ICBC (Europe) S.A.” 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.

This Special Section describes the risk relating to the Predicate Offenses concerning a fiscal/tax nature, therefore all the offenses referred to in Article 25-quinquiesdecies of Legislative Decree 231/01 in the conduct described above (with any relevant example) that may constitute or facilitate any type of conduct constituting a crime, by customers and through the Branch too.

The risk activities as identified within the activities of the Branch as well as the main safeguards aimed at preventing them from being carried out are listed below.

1.3.1 Management of the administrative and accounting structure and the authorization for the sale of significant assets and / or the approval of significant financial transactions.

The approval delegated powers of the Branch General Manager are specified in the annual internal operation and management authorization as granted and, from time to time, authorized by the ICBC (Europe) S.A. and are part in the decision-making process in the organizational settings and in the approval of significant activities, at a financial and fiscal level, for the Branch.

The General Manager of the Branch has per law authorization to organize and be liable for the organization of the Branch and shall report to ICBC (Europe) S.A. headquarters in Luxembourg.

The Parent Company supports the decision-making of the General Management and is in charge of performing any useful action or evaluation in order to verify and implement any relevant change in the organizational structure in order to prevent crimes too.

In this said context, among the activities at risk, the following measures have been implemented:

(a) the establishment and maintenance of the structure of the Accounting and Administration Departments which must always be maintained in an adequate structure (in terms of skills and organizational capacity) in compliance with the task performing and any adequate professional tax support.

The foregoing, in accordance with a preventive evaluation that has to be renewed periodically, is supported also by external tax consultants to allow full fiscal compliance of the Branch on an ongoing basis;

(b) the final approval of the main financial matters of the Branch and / or the implementation of financial projects (including cross-border transactions) that have a significant accounting or

tax effect for the Branch must always be supported as well as proceed by any adequate written assessments on the fiscal effect and in order to monitor compliance also in the following;

By way of example, these are all the activities that have a subsequent tax connection and a tax effect, depending on the relevant impact of tax compliance matters and evaluations, both on a declarative basis and/or concerning tax paying and/or having fiscal impacts to customers, depending on the same structure to fulfill tax obligations.

The following types of crimes are applicable in a theoretical way and the sensitive Predicated Offences:

I) Fraudulent declaration by other means (Art. 3 D. Lgs. No. 74/2000);

II) Issuing of invoices or other documents for non-existent transactions (Art. 8 D. Lgs. No. 74/2000);

III) Fraudulent subtraction from the payment of taxes (Article 11, Legislative Decree 74/2000);

IV) Undue compensation (Article 10-quater, Legislative Decree 74/2000).

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Special Part and in the General Part of the Model, are required to strictly observe and comply with the preventive measures provided for by the following internal regulations adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Staff Handbook
- Financial Accounting Manual and responsibilities of Financial Accounting Department
- Centralized Purchase rules;
- Treasury manual
- Banking Business Manual;
- Dac-6 procedures;
- CRS Manual
- Policies on the Management of External Legal Advisors;
- Credit management Manual;

- Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.2 Management of the proposition of new products, services or activities (authorization powers) of the Branch.

The Activities classified into the current section are considered submitted to a hierarchical and preventive approval.

The approval of delegated powers of the Branch General Manager is specified in the annual internal operation and management authorization as granted and, from time to time, authorized by ICBC (Europe) S.A. and is part of the decision-making process, of the organizational settings and of the approval of significant activities, at a financial and fiscal level, for the Branch.

The General Manager of the Branch has no authorization to approve new activities, products and/or banking services and shall report to ICBC (Europe) S.A. headquarters in Luxembourg for approval.

The Credit Committee supports the decision-making of the General Management in credit risk management and is in charge of performing any useful action or evaluation in order to verify the existing tax risk and/or any international mechanism that could create the potential commission of a tax crime.

In this said context, among the activities at risk, the following measures have been implemented:

(a) the approval and management (with the prior authorization of Headquarter as required) concerning any and all new activities and / or products.

In particular, for each new activity, product and / or service, the New Product Assessment Committee is entitled and required to and will assess the need for the prior release of any relevant legal and tax assessment to support the tax compliance (or the effect of changes resulting from new tax provisions);

(b) the approval of purchase and accounting and sale of significant financial assets;

(c) the approval of activities that involve the Branch in the renegotiation of commitments or obligations assumed and involving counterparties who may obtain undue tax advantages must be supported by suitable tax opinions.

By way of example, these are all the activities that have a tax connection and a potential tax effect, as direct and subsequent effect of the management of the tax risk relating to products and services offered to customers too (rif. marketing of banking and financial products and services too). In the latter case are included all situations in which transactions could qualify a potential involvement of the Branch, as a consequence the Branch must always be compliant in full with the best sector practices referring to and implementing tax provisions and do not have to be sentenced as facilitating tax evasion.

It is strictly encouraged that any tax activity and practice of the Branch are and shall always be in line with the general accounting policy and the best tax practices, and further must always be traceable and can be submitted to a documental reconstruction, as well as reasoned for any new product and/or activity and/or banking and financial service on tax effect to.

The following types of crimes are applicable in a theoretical way and the sensitive Predicated Offences:

I) Fraudulent declaration by other means (Art. 3 D. Lgs. No. 74/2000);

II) Issuing of invoices or other documents for non-existent transactions (Art. 8 D. Lgs. No. 74/2000);

III) Fraudulent subtraction from the payment of taxes (Article 11, Legislative Decree 74/2000);

IV) Undue compensation (Article 10-quater, Legislative Decree 74/2000).

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Special Part and in the General Part of the Model, are required to strictly observe and comply with the preventive measures provided for by the following internal regulations adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Staff Handbook
- Financial Accounting Manual and responsibilities of Financial Accounting Department
- Centralized Purchase rules;
- Treasury manual
- Banking Business Manual;
- Dac-6 procedures;
- New Product Assessment and Approval
- CRS Manual
- Policies on the Management of External Legal Advisors;
- Credit management Manual;
- AML & CTF - KYC Guidelines for the Milan Branch

- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding Procedure for Credit Institutions, Financial Institutions and Assimilated Financial institutions
- Suspicious Transaction Reporting procedure
- Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.3 Developing marketing and sales strategies

This risky Activity concerns activities related to:

- promoting the Branch's image to Italian market;
- Developing the marketing and sales strategies with a focus on growing the business volumes and customer base;
- Management of the relationship with prospective Corporate customers and any other type of counterparties;
- Arrangement of meetings with potential customers;
- Representing and promoting the Branch's image to niche market and local banking community.

In details, Marketing and Credit Management functions are performed by CIB Department and FI Department - as front office - and Risk Management Department respectively. The Marketing strategy and Credit Management activity and roles are performed independently by individuals.
The types of crime that are abstractly applicable and the related methods of committing them could concern an aggressive tax practice in favor of customer(s) and be connected to:

I. "Fraudulent declaration by other means" (Article 3 of Legislative Decree no. 74/2000).

Undue compensation (Article 10-quater, Legislative Decree 74/2000)..
By way of example, this kind of offense could be constituted if the Departments require and/or submit to authorization the entering into a customer relationship, on a willful basis, accepting (in an indirect way too) and/or offering illegal operations in order to facilitate the illicit purposes of the customer obtaining a benefit / interest, so that the Branch enters into a relationship that could generate an economic advantage in breach of law, committing an infringement 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 Special Part and in the General Part of the Model, are obliged to strictly observe the preventive measures included in the following internal regulation adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- Financial Accounting manual;
- Treasury Manual;
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Dac-6 procedures;
- Procedures for Credit Institutions, Financial Institutions and Assimilated Financial Institutions;
- Suspicious Transaction Reporting procedure.Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.4 Management of both the active and passive cycle of accounting and tax declarations.

The identified risk Activities concern those relating to the management of the active and passive cycle of accounting and may concern the Financial Accounting Department and the General Administration Department and are connected to:

- (in general) the full compliance with, even due to any organizational change and / or arising from new tax provisions, the general Financial and Accounting Manual (Including Income tax Code -Transfer pricing rules) and the Treasury Manual of the Branch;
- (in details) the management of the active cycle and the passive cycle of accounting in compliance with the tax provisions, time by time, in force;
- the correct and true execution of all declarative activities (of income and VAT) and / or timely settlement of taxes, contributions and / or taxes by the Branch (including the preparation and updating of the accounting manual and tax schedule);
- the management of the controls on accounting systems (operating and budget expenses and invoice and reimbursement and payment) of the Branch;
- the management of relations with the fiscal administration;
- the verification and monitoring on accounting data;
- the management control system;

- the operating expense management and the tax management implementing rules;
- the evaluation and management of the process for completing the annual audit.

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).

Listed below are the types of crime that are abstractly applicable and the related methods of commission:

I. Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000).

II. Fraudulent declaration through other devices (Article 3, Legislative Decree No. 74/2000).

III. Issue of invoices for non-existent transactions (Article 8, Legislative Decree No. 74/2000).

IV. Unfaithful declaration (Article 4, Legislative Decree 74/2000).

V. Omitted declaration (Article 5, Legislative Decree 74/2000).

VI. Undue compensation (Article 10-quater, Legislative Decree 74/2000.

VII. Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000).

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

- Code of Ethics
- Tax Management implementing rules;
- Code of Conduct of ICBC (Europe) S.A.
- Financial Accounting Manual;
- Treasury Manual;
- Internal Operation and Management Authorization
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and Procedure
- Staff Handbook
- Conflict of interest Policy
- Credit Management Manual
- Dac-6 procedures;
- Procedures for Credit Institutions, Financial Institutions and Assimilated Financial Institutions;
- Suspicious Transaction Reporting procedure.
- Anti Internal Fraud Policy

1.3.5 Management of the reliability and integrity of accounting and management expenses and information.

Concerning tax matters, the possibility of a subsequent reconstructing about the correct completion of any data or element having a fiscal effect that is the basis of and is included within the declaration and / or the settlement of the payment of taxes or duties is and must be qualified as sensitive and relevant.

All activities relating to the formation and reporting of costs and incomes, the proper and timely collection of accounting data, the preparation and drafting of reports concerning accounting data, also in order to certify their completeness and truthfulness, are considered to be sensitive and relevant.

By way of example, it could occur in carrying out any unlawful conduct, performed through and by any access to accounting systems too (both if performed by an unauthorized or by an authorized one) that cause the destruction, even partial, of accounting documentation and/or by altering or falsifying accounting documents used for tax declarations and/or obligation, having effect on costs, expenses, revenues.

Listed below are classified the types of crime that are applicable on an abstract basis and the related committing methods:

I. Concealment or destruction of documents and withdrawal from payment (art. 10, legislative

decree 74/2000).

The Recipients of the Model who operate in the context of this activity, in compliance with the general principles set out in the Special Part and in the General Part of the Model, are required to strictly observe and comply with the preventive measures provided for by the following internal regulations adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Staff Handbook
- Financial Accounting Manual and responsibilities of Financial Accounting Department
- Centralized Purchase rules;
- Treasury manual
- Dac-6 procedures
- Procedures for Credit Institutions, Financial Institutions and Assimilated Financial Institutions
- Suspicious Transaction Reporting procedure
- Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.6 Management of customer relations and operations.

Although the conduct typified in the Predicate Offenses are directly related to the commission of tax offenses by the Branch, conforming to international best practices, the Branch pursues the widest “fiscal compliance” .

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:

I. Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000).

II. Fraudulent declaration through other devices (Article 3, Legislative Decree No. 74/2000).

III. Unfaithful declaration (Article 4, Legislative Decree 74/2000).

IV. 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 Special Part and in the General Part of the Model, are required to strictly observe the preventive measures provided for by the following internal regulations adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Staff Handbook
- Banking Business Manual;
- Dac-6 procedures;
- CRS Manual

- Credit management Manual;
- AML & CTF – KYC Guidelines for the Milan Branch
- AML-CTF Due Diligence and Client Onboarding
- Suspicious Transaction Reporting procedure
- Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.7 Management of the reporting to the Tax Authority (including those provided by the international cooperation) and cross-border activities.

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 Special Part" - 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:

I. Fraudulent declaration through the use of invoices or other documents for non-existent operations (art. 2, legislative decree 74/2000).

II. Fraudulent declaration through other devices (Article 3, Legislative Decree No. 74/2000).

III. Fraudulent evasion of the payment of taxes (Article 11, Legislative Decree 74/2000).

IV. Unfaithful declaration (Article 4, Legislative Decree 74/2000).

V. 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 Special Part and in the General Part of the Model, are required to strictly observe the preventive measures provided for by the following internal regulations adopted by the Branch:

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A.
- Internal Operation and Management Authorization
- General Governance Policy of ICBC Milan Branch
- Staff Handbook
- Dac-6 procedures;
- New Product Assessment and Approval
- CRS Manual
- AML & CTF - KYC Guidelines for the Milan Branch
- AML & Compliance Committee Charter of ICBC (Europe) S.A. Milan Branch
- AML-CTF Due Diligence and Client Onboarding
- Suspicious Transaction Reporting procedure
- Anti-Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.8 Management of second level controls

As part of the verification of the so-called "Second level" checks it is increasingly necessary that specific "tax compliance" audits of the Branch's activities shall be carried out by the Financial and Accounting Department, also on and through the supplementary support provided by specific tax consultants, suggesting any corrective measures necessary to mitigate and / or prevent any risk of dispute of incorrect conduct and / or contrary to the provisions of the law.

As part of the checks and activities carried out by the Branch's Risk Management Department, it is relevant that the risks of tax non-compliance are considered, with reference to the identification, measurement, analysis, monitoring and periodic reporting of "tax compliance", as well as verifying the implementation of the suggestions issued by tax consultants.

Below, in accordance with the premise, the types of crime abstractly applicable in the sense indicated above are listed:

(1→) (art. 2 Legislative Decree no. 74/2000) "Fraudulent declaration through the use of invoices or other documents for non-existent operations".

(2→) (Article 3 of Legislative Decree no. 74/2000) "Fraudulent declaration by other devices".

(3→) Unfaithful declaration (Article 4 of Legislative Decree no. 74/2000) income tax, thus obtaining fraudulent savings for the company.

(4→) Omitted declaration (Article 5 of Legislative Decree No. 74/2000)

(5→) Issue of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000).

(6→) Concealment or destruction of accounting documents (Article 10 of Legislative Decree no. 74/2000).

(7→) Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000).

(8→) Undue compensation (Article 10-quater of Legislative Decree no. 74/2000).

By way of example, given the potentially transversal nature of a conduct or practice that is contrary or has become contrary to the law with the consequent effects also on tax settlement and payment declarations or activities, the offense can be configured as Activities of failure to identify conduct contrary to the law that do not correct conduct that involves the display of incorrect elements from the evaluation point of view as well as proceed to the active detection of omitted activities on tax obligations (declarations or payments).

The Recipients of the Model who operate within the scope of these risk control and measurement activities, in compliance with the general principles set out in the Special Part and in the General Part of the Model, are required to strictly comply with the preventive measures provided for by the following internal regulations adopted by Branch:

- Code of Ethics
- General Governance Policy of ICBC Milan Branch
- Code of Conduct of ICBC (Europe) S.A.
- Whistleblowing Policy and procedure
- Staff Handbook
- DAC-6
- Tax management Implementing rules
- CRS Manual

- Compliance Policy
- Milan Branch Enterprise-wide Risk Management Policy
- Conflict of interest Policy
- Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

1.3.9 Management of third level controls and audits.

The Internal Audit Department of the Branch is based at the Parent Company in Luxembourg and carries out the following activities annually, as part of third-level audits and controls:

- monitors the regular performance of transactions and the trend of risks (including tax);
- identifies anomalous trends, violations of procedures and regulations from a fiscal point of view;
- evaluates the completeness, adequacy, functionality and reliability of the organizational structure and of the other components of the internal control system (from the point of view of the correct fulfilment of tax obligations);
- brings to the attention of the corporate bodies any improvements in risk management policies and any critical issues or violations detected;
- based on the results of checks, it makes recommendations to the corporate bodies.

It is essential that, in the context of scheduled audits, attention and relevance is also paid to the verification of the "tax compliance" of the Branch on declaratory obligations and the settlement of tax taxes, as well as compliance with the fulfilment of international cooperation obligations.

Listed below are the types of crime that are abstractly applicable and the related methods of commission:

(1→) (art. 2 Legislative Decree no. 74/2000) "Fraudulent declaration through the use of invoices or other documents for non-existent operations".

(2→) (Article 3 of Legislative Decree no. 74/2000) "Fraudulent declaration by other devices".

(3→) Unfaithful declaration (Article 4 of Legislative Decree no. 74/2000)

(4→) Omitted declaration (Article 5 of Legislative Decree No. 74/2000)

(5→) Issue of invoices or other documents for non-existent transactions (Article 8 of Legislative Decree no. 74/2000).

(6→) Concealment or destruction of accounting documents (Article 10 of Legislative Decree no. 74/2000).

(7→) Fraudulent evasion of the payment of taxes (Article 11 of Legislative Decree no. 74/2000).

(8→) Undue compensation (Article 10-quater of Legislative Decree no. 74/2000).

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

- Code of Ethics
- Code of Conduct of ICBC (Europe) S.A
- General Governance Policy of ICBC (Europe) S.A. Milan Branch
- Whistleblowing Policy and procedure
- Internal Audit Charter of ICBC (Europe) S.A.
- Outsourcing Management Measures of ICBC (Europe) S.A. Milan Branch
- Anti Internal Fraud Policy
- Tax Affair Management Procedure of Milan Branch

ANNEXES

- Annex 1 - Matrix of Risks_ICBC (Europe) S.A. Milan Branch
- Annex 2 – List of Updated Predicated Offences